

# PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-222176

(43)Date of publication of application : 11.08.2000

(51)Int.Cl.

G06F 7/58

G06K 17/00

G06K 19/10

G09C 1/00

(21)Application number : 11-026369

(71)Applicant : MITSUBISHI ELECTRIC CORP  
MITSUBISHI DENKI SYSTEM LSI  
DESIGN KK

(22)Date of filing : 03.02.1999

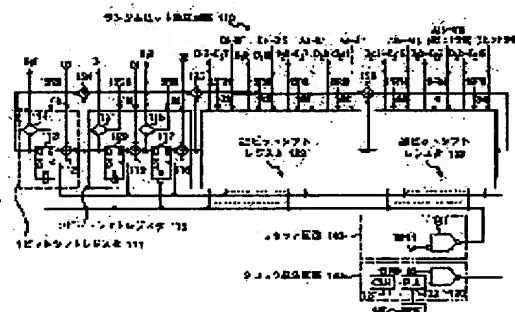
(72)Inventor : FUJIOKA SOZO

(54) RANDOM-NUMBER GENERATING CIRCUIT, NONCONTACT IC CARD AND READER/WRIter HAVING SAME RANDOM-NUMBER GENERATING CIRCUIT INSIDE, AND METHOD FOR TESTING DEVICE HAVING SAME RANDOM-NUMBER GENERATING CIRCUIT INSIDE

(57)Abstract:

**PROBLEM TO BE SOLVED:** To generate random number data which are irregular and hardly predicted and to generate the random number data fast with simple constitution by generating the random number data by making use of bit data sent through an external signal line.

**SOLUTION:** A random-bit generating circuit 110 adds bit data which changes with time according to process contents to be executed by a CPU to respective bit data stored in a 1-bit shift register 111, a 2-bit shift register 115, a 25-bit shift register 122, and a 20-bit shift register 123 constituting what is called a 48-bit M-series random number generating circuit. Namely, the respective bit data A0 to A19 of a 20-bit address signal sent through a system bus, the respective bit data D0 to D15 of a 16-bit data signal, and the respective bit data of 12 bits in total composed of other signals are added respectively. The 3 bytes obtained by the addition, i.e., data D10 to D115, D20 to D215, and D30 to D316 of 48 bits in total are outputted as random number data.



## LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

(19)



JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **2000222176 A**

(43) Date of publication of application: **11.08.00**

(51) Int. Cl.

**G06F 7/58**  
**G06K 17/00**  
**G06K 19/10**  
**G09C 1/00**

(21) Application number: **11026369**

(22) Date of filing: **03.02.99**

(71) Applicant: **mitsubishi electric  
corpmitsubishi denki  
system lsi design kk**

(72) Inventor: **FUJIOKA SOZO**

(54) **RANDOM-NUMBER GENERATING CIRCUIT,  
NONCONTACT IC CARD AND READER/WRITER  
HAVING SAME RANDOM-NUMBER GENERATING  
CIRCUIT INSIDE, AND METHOD FOR TESTING  
DEVICE HAVING SAME RANDOM-NUMBER  
GENERATING CIRCUIT INSIDE**

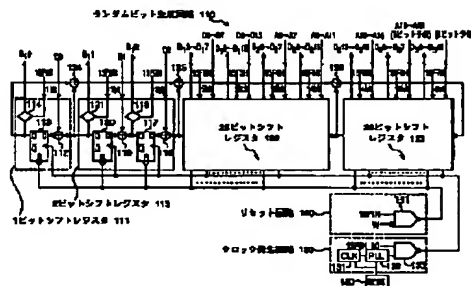
data of 12 bits in total composed of other signals are added respectively. The 3 bytes obtained by the addition, i.e., data D10 to D115, D20 to D215, and D30 to D316 of 48 bits in total are outputted as random number data.

COPYRIGHT: (C)2000,JPO

(57) Abstract:

PROBLEM TO BE SOLVED: To generate random number data which are irregular and hardly predicted and to generate the random number data fast with simple constitution by generating the random number data by making use of bit data sent through an external signal line.

SOLUTION: A random-bit generating circuit 110 adds bit data which changes with time according to process contents to be executed by a CPU to respective bit data stored in a 1-bit shift register 111, a 2-bit shift register 115, a 25-bit shift register 122, and a 20-bit shift register 123 constituting what is called a 48-bit M-series random number generating circuit. Namely, the respective bit data A0 to A19 of a 20-bit address signal sent through a system bus, the respective bit data D0 to D15 of a 16-bit data signal, and the respective bit



(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2000-222176

(P 2 0 0 0 - 2 2 2 1 7 6 A)

(43) 公開日 平成12年 8月11日 (2000.8.11)

(51) Int. Cl. <sup>7</sup>	識別記号	F I	テーマコード (参考)
G06F 7/58		G06F 7/58	A 5B035
G06K 17/00		G06K 17/00	T 5B058
19/10		G09C 1/00	B 5J104
G09C 1/00	650	G06K 19/00	R 9A001

審査請求 未請求 請求項の数 7 O L (全13頁)

(21) 出願番号 特願平11-26369

(22) 出願日 平成11年 2月 3日 (1999.2.3)

(71) 出願人 000006013

三菱電機株式会社

東京都千代田区丸の内二丁目 2番 3号

(71) 出願人 391024515

三菱電機システムエル・エス・アイ・デザイン株式会社

兵庫県伊丹市中央 3丁目 1番 17号

(72) 発明者 藤岡 宗三

兵庫県伊丹市中央 3丁目 1番 17号 三菱電機システムエル・エス・アイ・デザイン株式会社内

(74) 代理人 100062144

弁理士 青山 葆 (外 2名)

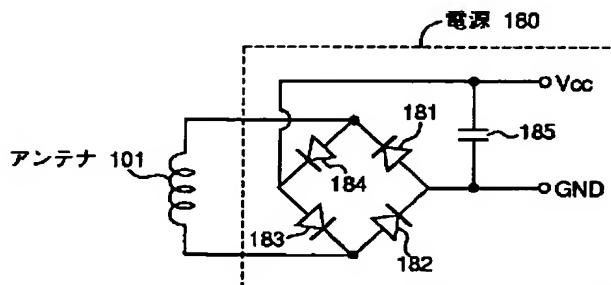
最終頁に続く

(54) 【発明の名称】 乱数生成回路、当該乱数生成回路を内蔵する非接触 I Cカード及びリーダ／ライタ、並びに、当該乱数生成回路を内蔵する装置のテスト方法

(57) 【要約】

【課題】 簡単な構成で、かつ、高速に精度の高い乱数を発生する乱数生成回路を提供する。

【解決手段】 本発明の乱数生成回路は、カスケード接続された 1 以上のビットのクロック同期型シフトレジスタと、上記複数のシフトレジスタの内の少なくとも 1 組のシフトレジスタの出力の合計を求め、求めた合計のデータを所定のシフトレジスタの入力端子に入力する加算回路と、上記各シフトレジスタにクロック信号を入力するクロック発生回路とで構成される乱数生成回路であって、上記複数のシフトレジスタの内の 1 以上のシフトレジスタは、格納しているビットデータの内の 1 以上のビットデータに外部信号線に流れるビットデータを加算する加算手段と、上記加算手段による加算後に、格納しているビットデータの内の 1 以上の所定のビットデータを乱数データとして出力する出力手段とを備えることを特徴とする。



## 【特許請求の範囲】

【請求項 1】 カスケード接続された複数のクロック同期型シフトレジスタと、上記複数のシフトレジスタの内の 2 以上のシフトレジスタの出力の合計を求め、求めた合計のデータを初段のシフトレジスタの入力端子に入力する回路と、上記各シフトレジスタにクロック信号を入力するクロック発生回路とを備え、各シフトレジスタの出力するビットデータを乱数データとして出力する乱数生成回路であって、

上記複数のシフトレジスタの内の 1 以上のシフトレジスタは、外部信号入力端子と、格納しているビットデータの内の 1 以上のビットデータに上記外部信号入力端子を介して入力されるビットデータを加算する加算回路とを備え、加算回路による加算後のビットデータを乱数データとして出力することを特徴とする乱数生成回路。

【請求項 2】 カスケード接続された複数のクロック同期型シフトレジスタと、上記複数のシフトレジスタの内の 2 以上のシフトレジスタの出力の合計を求め、求めた合計のデータを初段のシフトレジスタの入力端子に入力する回路と、上記各シフトレジスタにクロック信号を入力するクロック発生回路とを備え、各シフトレジスタの出力するビットデータを乱数データとして出力する乱数生成回路であって、

上記クロック発生回路は、所定の周波数のクロック信号を生成する CLK 回路と、上記 CLK 回路により生成されたクロック信号を基準周波数信号として受け取る PLL 回路とで構成され、上記 PLL 回路の出力を上記各シフトレジスタに出力することを特徴とする乱数生成回路。

【請求項 3】 請求項 1 又は請求項 2 に記載の乱数生成回路において、

上記シフトレジスタを構成するクロック同期型のフリップフロップは、電源投入時に出力するデータを "H" とする第 1 構成要素と、第 1 構成要素と同一のドライブ能力を有し、電源投入時に出力するデータを "L" とする第 2 構成要素とを備え、上記第 1 及び第 2 構成要素の出力端子には、それぞれ同一の容量の配線及びトランジスタが接続されていることを特徴とする乱数生成回路。

【請求項 4】 請求項 1 乃至請求項 3 の何れかに記載の乱数生成回路において、

更に、リセット要求信号の入力に応じて各シフトレジスタにリセット信号を出力するリセット回路を備え、上記クロック発生回路は、クロック停止信号の入力に応じてクロック信号の各シフトレジスタへの出力を停止し、クロック動作信号の入力に応じてクロック信号を各シフトレジスタへ出力する論理回路を備えることを特徴とする乱数生成回路。

【請求項 5】 請求項 1 乃至請求項 4 の何れかに記載の乱数生成回路を内蔵する非接触 IC カードであって、当該非接触 IC カード用リーダ／ライタとの間で、上記内

蔵する乱数生成回路から出力される乱数データを用いて通信処理を実行する制御手段を備え、上記制御手段により使用される所定の信号線が上記外部信号入力端子に接続されていることを特徴とする非接触 IC カード。

【請求項 6】 請求項 1 乃至請求項 4 の何れかに記載の乱数生成回路を内蔵する非接触 IC カード用リーダ／ライタであって、対応する非接触 IC カードとの間で、上記内蔵する乱数生成回路から出力される乱数データを用いて通信処理を実行する制御手段を備え、上記制御手段により使用される所定の信号線が上記外部信号入力端子に接続されていることを特徴とする非接触 IC カード用リーダ／ライタ。

【請求項 7】 請求項 4 に記載の乱数生成回路を内蔵し、当該内蔵する乱数生成回路から出力される乱数データを用いて所定の処理を実行する制御手段を備え、上記制御手段により使用される所定の信号線が上記外部信号入力端子に接続されている装置のテスト方法であって、クロック発生回路から所定の周波数のクロック信号が出力されている状態において、クロック発生回路の論理回路にクロック停止信号を出力し、リセット回路にリセット要求信号を出力した後に、クロック発生回路の論理回路にクロック動作信号を出力すると同時に上記装置のテスト処理を実行し、上記テスト処理の完了と同時にクロック発生回路の論理回路にクロック停止信号を出力し、出力手段より出力される乱数データの値を読み取り、読み取った乱数データと基準データとの比較により、システムの異常検出を行うことを特徴とする装置のテスト方法。

## 【発明の詳細な説明】

## 【 0 0 0 1 】

【発明の属する技術分野】 本発明は、乱数生成回路、特に、非接触 IC カード及び当該非接触 IC カードのリーダ／ライタに用いる乱数生成回路に関する。

## 【 0 0 0 2 】

【従来の技術】 近年、インテリジェント機能や書き換え可能なメモリ機能を備える薄型の非接触 IC カードが数多く提供されている。非接触 IC カードは、リーダ／ライタに接続させることなくデータのやり取りができることを特徴とする。非接触 IC カードは、例えば、プリペイドカード、ドアの鍵、電車やバスなどの定期券、スキーのリフト券等に用いられる。

【 0 0 0 3 】 非接触 IC カードに書き込まれているデータの不正流出や改竄を防止するため、上記非接触 IC カードと当該カードのリーダ／ライタは、データのやり取りを行う前に、互いを認証する処理を実行する。リーダ／ライタは、自己の発信するポーリング信号に対して所定のレスポンス信号を返信してきた非接触 IC カードとの間で相互認証処理を実行する。相互認証処理の方法としては、暗号化鍵を用いる方法が知られている。

## 【 0 0 0 4 】 以下、非接触 IC カードとリーダ／ライタ

との間で行う暗号を用いた相互認証処理について簡単に説明する。まず、リーダ／ライタは、非接触 IC カードに対して内部で生成した乱数  $a$  を送信する。非接触 IC カードは、受信した乱数  $a$  を自己の暗号化鍵を用いて乱数  $A$  に変換し、乱数  $A$  をリーダ／ライタに返送する。リーダ／ライタでは、特定の非接触 IC カードとの間で用いる共通の暗号化鍵を用いて上記生成した乱数  $a$  を処理して乱数  $A'$  を求め、求めた乱数  $A'$  と上記非接触 IC カードから返送されてきた乱数  $A$  とを比較する。リーダ／ライタは、乱数  $A$  と乱数  $A'$  が一致する場合に当該非接触 IC カードを正規のものであると認証する。

【0005】次に、非接触 IC カードはリーダ／ライタに対して内部で生成した乱数  $b$  を送信する。この場合、リーダ／ライタは、受信した乱数  $b$  を自己の暗号化鍵を用いて乱数  $B$  に変換し、乱数  $B$  を非接触 IC カードに返送する。非接触 IC カードは、特定のリーダ／ライタとの間で用いる共通の暗号化鍵を用いて上記生成した乱数  $b$  を処理して乱数  $B'$  を求め、求めた乱数  $B'$  と上記リーダ／ライタから返送されてきた乱数  $B$  とを比較する。非接触 IC カードは、乱数  $B$  と乱数  $B'$  が一致する場合に当該リーダ／ライタを正規のものであると認証する。

【0006】非接触 IC カード及びリーダ／ライタ内には上記相互認証処理で用いる乱数を生成する乱数生成回路が内蔵されている。図 10 は、従来より用いられている乱数生成回路 500 の回路図である。乱数生成回路 500 は、いわゆる 48 ビット M 系列乱数生成回路と呼ばれる回路であり、カスケード（多段直列）接続された 1 ビットシフトレジスタ 501、2 ビットシフトレジスタ 504、25 ビットシフトレジスタ 505 及び 20 ビットシフトレジスタ 506、並びに、各ビットシフトレジスタの出力の合計を初段の 20 ビットシフトレジスタ 506 の入力端子に入力する加算回路を構成する加算器 507、508 及び 509 で構成される。

【0007】1 ビットシフトレジスタ 501 は、CLK 回路 510 より出力されるクロック信号 CLK に同期して動作するフリップフロップ 502 及びトランスファゲート 503 により構成される。図示しない CPU によりアドレス 02EH が選択されアドレス信号線が“L”から“H”に切り換わった時にフリップフロップ 502 の出力を乱数データ  $D_1 0$  として出力する。

【0008】2 ビットシフトレジスタ 504、25 ビットシフトレジスタ 505 及び 20 ビットシフトレジスタ 506 の回路は、各々シフトするビット数だけ上記 1 ビットシフトレジスタ 501 と同じ回路を直列に接続したものである。2 ビットシフトレジスタ 504 は、アドレス 15F2H が選択された時に乱数データ  $D_1 1$ 、 $D_1 2$  を出力する。25 ビットシフトレジスタ 505 は、アドレス 15F2H、15F3H、15F4H 及び 15F5H が選択された時に乱数データ  $D_1 3 \sim D_1 7$ 、 $D_1 8 \sim D_1 15$ 、 $D_1 0 \sim D_1 7$  及び  $D_1 8 \sim D_1 11$  を出力す

る。20 ビットシフトレジスタ 506 は、アドレス 15F5H、15F6H 及び 15F7H が選択された時に乱数データ  $D_1 12 \sim D_1 15$ 、 $D_1 0 \sim D_1 7$ 、 $D_1 8 \sim D_1 15$  を出力する。

【0009】

【発明が解決しようとする課題】上記構成の乱数生成回路 500 の生成する乱数は、一定の周期で繰り返す所定の生成パターンを有する。このため、リーダ／ライタと非接触 IC カードとの間でやり取りされる通信データが盗聴され、乱数の生成パターンが特定される場合がある。このように乱数の生成パターンが特定されると、暗号化鍵や暗号化処理の内容が解らずとも、乱数  $a$  と乱数  $A$  を対応づけたテーブルを用いることで非接触 IC カードを偽造することができる。同様に、乱数  $b$  と乱数  $B$  を対応づけたテーブルを用いることでリーダ／ライタの偽造を行うことができる。

【0010】上記通信データの盗聴による非接触 IC カードやリーダ／ライタの偽造を有効に防止するには、通信データを盗聴しても生成パターンを解読できない程の高度な乱数生成回路が要求される。しかし、乱数生成回路を複雑化すれば乱数生成パターンの不正な解読を有効に防止することができるが、回路のサイズが大きくなってしまう。特に非接触 IC カードの場合、内蔵する乱数生成回路のサイズは小さいほうが好ましい。

【0011】非接触 IC カードは、リーダ／ライタと通信可能な領域にある間に相互認証処理を含む通信処理を完了する必要がある。このため、スロットに差し込んで使用する IC カードよりも高速な通信処理の実行が要求される。また、非接触 IC カードの場合、リーダ／ライタと通信可能な領域内に同時に複数の非接触 IC カードが入り込むことがある。この場合、各非接触 IC カードは、上記相互認証処理を含む通信処理の実行前に、例えば内部で生成した乱数に基づくタイミングでリーダ／ライタからのポーリング信号に対するレスポンス信号を出力する等、他の非接触 IC カードから出力されるレスポンス信号との衝突を回避する処理を実行する必要がある。非接触 IC カードとリーダ／ライタ間の通信速度を向上するには、高速で動作する乱数生成回路が要求される。

【0012】本発明は、簡単な構成で当該回路を内蔵する装置の小型化に寄与し、かつ、高速に規則性の無い予測の困難な乱数データを発生する乱数生成回路、当該乱数生成回路を内蔵する非接触 IC カード、及び、当該乱数生成回路を内蔵する非接触 IC カード用リーダ／ライタを提供することを目的とする。

【0013】

【課題を解決するための手段】本発明の第 1 の乱数生成回路は、カスケード接続された複数のクロック同期型シフトレジスタと、上記複数のシフトレジスタの内の 2 以上のシフトレジスタの出力の合計を求め、求めた合計の

データを初段のシフトレジスタの入力端子に入力する回路と、上記各シフトレジスタにクロック信号を入力するクロック発生回路とを備え、各シフトレジスタの出力するビットデータを乱数データとして出力する乱数生成回路であって、上記複数のシフトレジスタの内の 1 以上のシフトレジスタは、外部信号入力端子と、格納しているビットデータの内の 1 以上のビットデータに上記外部信号入力端子を介して入力されるビットデータを加算する加算回路とを備え、加算回路による加算後のビットデータを乱数データとして出力することを特徴とする。

【0014】本発明の第 2 の乱数生成回路は、カスケード接続された複数のクロック同期型シフトレジスタと、上記複数のシフトレジスタの内の 2 以上のシフトレジスタの出力の合計を求め、求めた合計のデータを初段のシフトレジスタの入力端子に入力する回路と、上記各シフトレジスタにクロック信号を入力するクロック発生回路とを備え、各シフトレジスタの出力するビットデータを乱数データとして出力する乱数生成回路であって、上記クロック発生回路は、所定の周波数のクロック信号を生成する CLK 回路と、上記 CLK 回路により生成されたクロック信号を基準周波数信号として受け取る PLL 回路とで構成され、上記 PLL 回路の出力を上記各シフトレジスタに出力することを特徴とする。

【0015】本発明の第 3 の乱数生成回路は、上記第 1 又は第 2 の乱数生成回路において、上記シフトレジスタを構成するクロック同期型のフリップフロップは、電源投入時に出力するデータを”H”とする第 1 構成要素と、第 1 構成要素と同一のドライブ能力を有し電源投入時に出力するデータを”L”とする第 2 構成要素とを備え、上記第 1 及び第 2 構成要素の出力端子には、それぞれ同一の容量の配線及びトランジスタが接続されていることを特徴とする。

【0016】本発明の第 4 の乱数生成回路は、上記第 1 乃至第 3 の何れかの乱数生成回路において、更に、リセット要求信号の入力に応じて各シフトレジスタにリセット信号を出力するリセット回路を備え、上記クロック発生回路は、クロック停止信号の入力に応じてクロック信号の各シフトレジスタへの出力を停止し、クロック動作信号の入力に応じてクロック信号を各シフトレジスタへ出力する論理回路を備えることを特徴とする。

【0017】本発明の非接触 IC カードは、上記第 1 乃至第 4 の何れかの乱数生成回路を内蔵する非接触 IC カードであって、当該非接触 IC カード用リーダ／ライタとの間で、上記内蔵する乱数生成回路から出力される乱数データを用いて通信処理を実行する制御手段を備え、上記制御手段により使用される所定の信号線が上記外部信号入力端子に接続されていることを特徴とする。

【0018】本発明のリーダ／ライタは、上記第 1 乃至第 4 の何れかの乱数生成回路を内蔵する、非接触 IC カード用リーダ／ライタであって、対応する非接触 IC カ

ードとの間で、上記内蔵する乱数生成回路から出力される乱数データを用いて通信処理を実行する制御手段を備え、上記制御手段により使用される所定の信号線が上記外部信号入力端子に接続されていることを特徴とする。

【0019】上記第 4 の乱数生成回路を内蔵し、当該内蔵する乱数生成回路から出力される乱数データを用いて所定の処理を実行する制御手段を備え、上記制御手段により使用される所定の信号線が上記外部信号入力端子に接続されている装置のテスト方法であって、クロック発生回路の論理回路にクロック停止信号を出力すると共に、リセット回路にリセット要求信号を出力した後に、クロック発生回路の論理回路にクロック動作信号を出力すると同時に上記装置のテスト処理を実行し、上記テスト処理の完了と同時にクロック発生回路の論理回路にクロック停止信号を出力し、出力手段より出力される乱数データの値を読み取り、読み取った乱数データと基準データとの比較により、システムの異常検出を行い、上記内蔵する乱数生成回路をテスト回路として利用する。これにより、テスト専用の回路を不要にして装置の小型化を図ることができる。

【0020】

【発明の実施の形態】以下、実施の形態に係る乱数生成回路、当該乱数生成回路を内蔵する非接触 IC カード、及び、当該乱数生成回路を内蔵する非接触 IC カード用リーダ／ライタについて、添付の図面を参照しつつ説明する。

【0021】(1) 非接触 IC カード

本実施の形態に係る乱数生成回路を内蔵する非接触 IC カードは、例えば、地下鉄の自動改札システムに採用することを想定している。より具体的には、図 1 に示すように、自動改札機として機能するリーダ／ライタ 400 の前を、例えば定期券や回数券としての機能を有する非接触 IC カード 100、200、300 を有する人が順に通過する場合を想定する。リーダ／ライタ 400 は、前を通過する際に通信エリア内に入る非接触 IC カード 100、200、300 を順に認識し、定期券か回数券の種別についての情報、カードが定期券の場合には有効期限などの情報、及び、カードが回数券の場合には残りの枚数などの情報を読み取り、更に、必要に応じて各カードの情報を更新する。

【0022】(2) 非接触 IC カードの認証

リーダ／ライタ 400 は、自己の発信するポーリング信号に対して所定のレスポンス信号を返信してきた非接触 IC カードとの間で相互認証処理を実行する。図 2 は、非接触 IC カード 100 とリーダ／ライタ 400 との間で行われる相互認証処理のシーケンスを示す図である。まず、リーダ／ライタ 400 から非接触 IC カード 100 に対して内蔵する乱数生成回路により生成した認証用乱数 a を送信する（ステップ S1）。通信エリア内において認証用乱数 a を受信した非接触 IC カード 100

10

20

30

40

50

は、自己の暗号化鍵を用いて乱数aを乱数Aに変換し、乱数Aをリーダ/ライタ400に対して返信すると共に、内蔵する乱数生成回路により生成した認証用乱数bを送信する(ステップS2)。リーダ/ライタ400は、アクセスを行う非接触ICカードと共通に用いる暗号化鍵を用いて乱数aを乱数A'に変換し、乱数A'と非接触ICカード100から返信されてきた乱数Aとが一致する場合に非接触ICカード100を認証する。また、非接触ICカード100より送信されてきた乱数bを自己の暗号化鍵を用いて乱数Bに変換し、乱数Bを非接触ICカード100に対して返信する(ステップS3)。非接触ICカード100は、アクセスを行うリーダ/ライタと共通に用いる暗号化鍵を用いて乱数bを乱数B'に変換し、乱数B'と返信されてきた乱数Bとが一致する場合にリーダ/ライタ400を認証する(ステップS4)。

【0023】(3) 非接触ICカード及びリーダ/ライタの構成

図3は、非接触ICカード100及びリーダ/ライタ400のブロック構成図である。なお、非接触ICカード200、300の構成は、非接触ICカード100と同じであり、重複した説明は省略する。

【0024】非接触ICカード100は、電池レスタイプの非接触ICカードである。電源回路180は、リーダ/ライタ400から送信される高周波信号をアンテナ101により受信し、受信した高周波信号を整流して得られる信号を電圧Vccの供給信号としてクロック発生回路130を含む各内部回路に供給する。電源回路180の構成については後に説明する。

【0025】クロック発生回路130は、上記電源回路180から供給される電圧Vccにより駆動され、クロック信号CLKを中央演算処理装置であるCPU103、乱数生成回路107を構成するランダムビット生成回路110、及び、その他の回路素子に出力する。クロック発生回路130の構成については後に説明する。

【0026】CPU103には、システムバス170を介して送受信回路102、ROM104、RAM105、情報記憶部106、及び、乱数生成回路107が接続されている。送受信回路102は、アンテナ101に接続されており、CPU103から送られてくる命令やデータを載せた高周波信号をアンテナ101を介して外部に発信すると共に、アンテナ101を介して受信した高周波信号から命令やデータを抽出してCPU103に出力する処理を行う。ROM104は、リーダ/ライタ400との相互認証処理等の通信処理を実行するプログラムを格納する。RAM105は、ROM104に格納するプログラムのCPU103による実行時に使用される。情報記憶部106は、独自の情報、例えば非接触ICカード100が定期券として機能する場合、カードの有効期限や有効乗車エリアなどの固有の情報を保持す

る。CPU103は、リーダ/ライタ400との通信処理の実行に伴い、必要に応じて上記情報記憶部106に記憶する情報の更新を行う。乱数生成回路107は、CPU103による所定のアドレスの選択に応じてリーダ/ライタ400との相互認証処理等で用いる乱数データを上記CPU103に出力する。

【0027】乱数生成回路107は、デコーダ108、ランダムビット生成回路110及びリセット回路140で構成される。デコーダ108は、CPU103のシステムバス170を介して入力されるアドレス信号のデータをデコードしてランダムビット生成回路110に出力する。ランダムビット生成回路110は、システムバス170に流れるアドレス信号のデータ、データ信号のデータ及びその他の信号のデータが内部で生成する乱数データを複雑化するために入力され、上記デコーダ108を介して所定のアドレスの選択された場合に合計で3バイト(48ビット)の乱数データをCPU103に出力する。リセット回路140は、CPU103の制御に応じて所定のリセット信号をランダムビット生成回路140に出力する。なお、ランダムビット生成回路110及びリセット回路140の構成については後に詳しく説明する。

【0028】リーダ/ライタ400は、アンテナ401、上記アンテナ401を用いて命令やデータが載った高周波信号の送受信を行う送受信回路402、中央演算処理装置であるCPU403、上記非接触ICカード100との相互認証処理を含む通信プログラムを格納しているROM404、CPU403によるプログラム実行時に使用されるRAM405、インターフェース406、及び、乱数生成回路407より構成される。なお、乱数生成回路407は、非接触ICカード100に内蔵する乱数生成回路107と同じ構成である。

【0029】リーダ/ライタ400において、中央演算処理装置であるCPU403は、システムバスを介して送受信回路402、ROM404、RAM405、インターフェース406及び乱数生成回路407に接続されている。送受信回路402は、接続されるアンテナ401を介して受信した高周波信号から命令やデータを抽出してCPU403に出力すると共に、CPU403からの命令やデータを載せた高周波信号をアンテナ401を介して発信する。CPU403は、例えば非接触ICカード100との相互認証処理の実行時に、乱数生成回路407から得られる乱数データを用いる。CPU403は、通信処理の結果をインターフェース406を介して各処理装置へ出力する。

【0030】図4は、電源回路180の構成を示す図である。電源回路180は、整流回路を構成するダイオード181、182、183及び184、並びに、容量185で構成される。当該整流回路は、アンテナ101を介して入力される高周波信号の整流を行い、当該整流後

の信号を電圧供給信号として各内部回路に出力する。

【0031】図5は、リーダ／ライタ400からの高周波信号の受信開始から電源回路180から出力される電圧供給信号の電位の変化を示すグラフである。図示するように、電源回路180から出力される電圧供給信号の電位が規定値Vccになるには、高周波信号の受信を開始してから所定の時間が必要である。なお、電圧供給信号の電位がVccとなるまでに要する時間は、リーダ／ライタ400との通信環境により変化する。

#### 【0032】(4) 乱数生成回路

図6は、乱数生成回路107に内蔵されるランダムビット生成回路110及びリセット回路140、並びに、クロック発生回路130の詳細な構成を示す図である。

#### 【0033】(4-1)ランダムビット生成回路

ランダムビット生成回路110は、いわゆる48ビットM系列乱数生成回路を構成する1ビットシフトレジスタ111、2ビットシフトレジスタ115、25ビットシフトレジスタ122、及び、20ビットシフトレジスタ123に格納される各ビットデータに、CPU103の実行する処理の内容により時間と共に変化するビットデータ、具体的には、システムバス170を通る20ビットのアドレス信号の各ビットデータA0～A19、16ビットのデータ信号の各ビットデータD0～D15、及び、その他の信号で構成される計12ビットの各ビットデータを各々加算し、加算して得られる3バイト、即ち計48ビットのデータD<sub>i</sub>0～D<sub>i</sub>15、D<sub>i</sub>0～D<sub>i</sub>15、D<sub>i</sub>0～D<sub>i</sub>15を乱数データとして出力する構成を採用したことを特徴とする。

【0034】上記構成を採用することで、規則性の無い予測の困難な乱数データを生成することができる。これにより、非接触ICカード100とリーダ／ライタ400との間で行われる通信データを盗聴しても乱数の生成パターンを特定することが難しくなり、非接触ICカードの偽造を有効に防止することができる。また、ランダムビット生成回路110は、シフトレジスタ及び加算器(XORゲート)を接続しただけの簡単な構成を採用するため、高速な乱数の生成を行うことができる。

【0035】以下、ランダムビット生成回路110の構成について詳説する。ランダムビット生成回路110は、カスケード(多段直列)接続された1ビットシフトレジスタ111、2ビットシフトレジスタ115、25ビットシフトレジスタ122及び20ビットシフトレジスタ123、並びに、各シフトレジスタの出力の合計を初段の20ビットシフトレジスタ123に出力する回路を構成する3つの加算器124、125、126で構成される。

【0036】20ビットシフトレジスタ123の入力端子は加算器126の出力端子に接続される。20ビットシフトレジスタ123の出力端子は加算器126の入力端子及び25ビットシフトレジスタ122の入力端子に

接続される。25ビットシフトレジスタ122の出力端子は、加算器125の入力端子及び2ビットシフトレジスタ115の入力端子に接続される。2ビットシフトレジスタ115の出力端子は、加算器124の入力端子及び1ビットシフトレジスタ111の入力端子に接続される。1ビットシフトレジスタ111の出力端子は、加算器124の入力端子に接続される。加算器124の出力端子は加算器125の入力端子に接続される。加算器125の出力端子は加算器126の入力端子に接続される。

【0037】1ビットシフトレジスタ111は、デコーダ108を介してアドレス15F2Hが選択され、対応するアドレス信号線が”L”から”H”に切り換わった時に、格納する1ビットデータに、システムバス170を流れる16ビットのデータ信号のbit0のデータD<sub>i</sub>0を加算して得られるデータのbit0のデータD<sub>i</sub>0を乱数データとして出力する。

【0038】1ビットシフトレジスタ111は、加算器112、フリップフロップ113、トランスファゲート114で構成されている。加算器112は、例えばEXORゲートで構成され、前段に設けられる2ビットシフトレジスタ115の出力に、システムバス170を介して入力される16ビットデータ信号のbit0のデータD<sub>i</sub>0を加算して得られるbit0のデータをフリップフロップ113に入力する。フリップフロップ113は、クロック同期型のフリップフロップであり、クロック入力端子に入力されるクロック信号CLKの遷移タイミングに同期して動作する。トランスファゲート114は、アドレス15F2Hが選択され、対応するアドレス信号線が”L”から”H”に切り換わった時に、フリップフロップ113の出力Qを乱数データD<sub>i</sub>0として出力する。

【0039】2ビットシフトレジスタ115は、デコーダ108を介してアドレス15F2Hが選択され、対応するアドレス信号線が”L”から”H”に切り換わった時に、格納している2ビットの各ビットデータに、データバスを介して入力される16ビットデータ信号のbit2のデータD<sub>i</sub>2及びbit1のデータD<sub>i</sub>1を加算したデータD<sub>i</sub>1及びD<sub>i</sub>2を乱数データとして出力する。

【0040】図示するように、2ビットシフトレジスタ115は、1ビットシフトレジスタを2段直列に接続したものである。即ち、加算器116、フリップフロップ117、及び、トランスファゲート118で1つ目の1ビットシフトレジスタを構成し、次の加算器119、フリップフロップ120、及び、トランスファゲート121で2つ目の1ビットシフトレジスタを構成する。以下に説明する25ビットシフトレジスタ122及び20ビットシフトレジスタ123も同様である。各シフトレジスタ内における信号の処理内容は上記1ビットシフトレジスタ111と同様であるため、ここでの説明は省

略する。

【0041】25ビットシフトレジスタ122は、格納している25ビットの各ビットデータに、アドレスバスを介して入力される20ビットのアドレス信号のbit 0～bit 11の各ビットデータA0～A11、及び、データバスを介して入力される16ビットのデータ信号のbit 3～bit 15の各ビットデータD3～D15を加算して得られる25ビットのビットデータD<sub>i</sub> 3～D<sub>i</sub> 7, D<sub>i</sub> 8～D<sub>i</sub> 15, D<sub>i</sub> 0～D<sub>i</sub> 7及びD<sub>i</sub> 8～D<sub>i</sub> 11を、アドレス15F2H, 15F3H, 15F4H 10及び15F5Hの選択に応じて出力する。

【0042】20ビットシフトレジスタ123は、格納されている20ビットの各ビットデータに、データ信号及びアドレス信号以外の信号で構成される8ビットの各ビットデータbit 0～bit 7の各ビットデータRev 0～Rev 7、及び、アドレスバスを介して入力される20ビットのアドレス信号のbit 12～bit 19の各ビットデータA12～A19を加算した20ビットのデータD<sub>i</sub> 12～D<sub>i</sub> 15, D<sub>i</sub> 0～D<sub>i</sub> 7及びD<sub>i</sub> 8～D<sub>i</sub> 15を、アドレス15F5H, 15F6H及び15 20F7Hの選択に応じて出力する。

【0043】上述するように、ランダムビット生成回路110では、各ビットシフトレジスタ111, 115, 122及び123内に格納する各ビットデータに対して、システムバス170を流れるアドレス信号、データ信号及びその他の信号を構成する各ビットデータを加算する構成を採用する。システムバス170に流れる信号の値は、実行する処理内容に伴い種々変化するため、規則性の無い予測の困難な乱数データを生成することができる。これにより、非接触ICカード100とリーダ/ライタ400との間で交わされる通信データを盗聴しても乱数の生成パターンを特定することは難しくなり、非接触ICカードの偽造を有効に防止することができる。また、ランダムビット生成回路110は、シフトレジスタ及び加算器（EXORゲート）を接続しただけの簡単な構成であるため、高速な乱数の生成を行うことができる。

【0044】上記ランダムビット生成回路110は、カスケード接続した全てのシフトレジスタの出力の合計を初段の20ビットシフトレジスタ123の入力端子に入力する構成を採用するが、これに限定されず、ランダムビット生成回路110を構成する4つのシフトレジスタの内の2以上のシフトレジスタの出力の合計を初段の20ビットシフトレジスタ123の入力端子に入力する構成であれば良い。

【0045】また、ランダムビット生成回路110は、CPU103による所定のアドレスの選択に対応して全てのシフトレジスタに格納するビットデータを乱数データとして出力する構成を採用するが、これに限定されず、1以上のビットデータを出力する構成であれば良

い。

【0046】更に、ランダムビット生成回路110は、各シフトレジスタに格納する全てのビットデータにシステムバス170のビットデータを加算する構成を採用しているが、これに限定されず、シフトレジスタに格納しているビットデータの内の1以上のビットデータにシステムバス170のビットデータを加算する構成であれば良い。

【0047】(4-2)リセット回路

リセット回路140は、2入力NANDゲート141で構成される。NANDゲート141の入力端子にはアドレス15F1Hのアドレス信号線が接続され、残りの入力端子には書き込み命令が出された場合に”L”から”H”に切り換わるW信号線が接続されている。CPU103は、アドレス15F1Hに対してデータの書き込みを行うことで、ランダムビット生成回路110を構成する各シフトレジスタ111, 115, 122, 123のリセットを行うことができる。

【0048】(4-3)クロック発生回路

図6に示すように、クロック発生回路130は、CLK回路131、PLL132、及び、NANDゲート133で構成される。CLK回路131は、電源回路180から電圧供給信号が出力されると同時に、所定の周期のクロック信号を基準周波数信号として次段のPLL回路132に出力する。周知のように、PLL回路132は、上記基準周波数信号の周波数に収束するまでの間、電源回路180から出力される電圧供給信号の電位に比例して決まる周波数のクロック信号を出力する。PLL回路132の出力端子は、2入力NANDゲート133の一方の入力端子に接続されている。NANDゲート133のもう一方の入力端子には、デコード後のアドレス15F0Hのbit 0のデータb0が入力される。通常、アドレス15F0Hのデータb0は”L”に設定されており、NANDゲート133は、PLL回路131からのクロック信号CLKの反転信号をランダムビット生成回路110を構成する各シフトレジスタ111, 115, 122及び123に出力する。

【0049】上述するように、クロック発生回路130の出力するクロック信号の周波数は、電源回路180から出力される電圧供給信号の電位により決まる。このため、電源回路180から出力される電圧供給信号の電位が規定値V<sub>cc</sub>に安定するまでの間は、全く同じタイミングで乱数データの読み取りを行っても、ランダムビット生成回路110から出力される乱数データの値は異なる。また、非接触ICカード100と全く同じ構成の非接触ICカード200や300であっても、各構成部品のばらつきにより上記乱数データの読み取りタイミングは微妙に異なるため、電源投入直後にランダムビット生成回路110から出力される乱数データは各カード毎に異なる。このように上記構成のクロック発生回路130

を採用することで、通信データの盗聴による乱数データの発生パターンの特定を一層難しくすることができる。

【0050】なお、上記構成のクロック発生回路130において、CPU103によりアドレス15F0Hのbit0のデータb0が”L”から”H”に書き換えられると、NANDゲート133は”H”のみを出力する。これにより、ランダムビット生成回路110を構成する各シフトレジスタ111、115、122及び123へのクロック信号の出力は停止し、各シフトレジスタの機能は停止する。また、アドレス15F0Hのbit0のデータb0の値を”H”から”L”に書き換えることで、各シフトレジスタへのクロック信号の出力を再開することができる。このように、CPU103は、ランダムビット生成回路110を動作及び停止することができる。

#### 【0051】(4-4)フリップフロップ

1ビットシフトレジスタ111を構成するクロック同期型フリップフロップ113は、電源投入時に出力するデータを”H”とする第1構成要素と、上記第1構成要素と同じドライブ能力を備え、電源投入時に出力するデータを”L”とする第2構成要素を備えると共に、上記第1及び第2構成要素の出力端子に接続される配線容量を同じにしたことを特徴とする。これにより、電源投入時に出力されるデータが”H”又は”L”となる確率を50%にする。

【0052】図7は、フリップフロップ113の構成を示す図である。2入力ORゲート150の一方の入力端子は、クロック信号CLKの入力端子に接続されており、他方の入力端子はデータ信号Dの入力端子に接続されている。ORゲート150の出力端子は2入力NANDゲート151の一方の入力端子に接続されている。NANDゲート151の出力端子は、2入力NANDゲート153の一方の入力端子、ゲート電極及びソース電極が接地されているNチャンネルMOSトランジスタ159のドレイン電極、及び、2入力ANDゲート154の一方の入力端子に接続されている。2入力ORゲート152の一方の入力端子は、クロック信号CLKの入力端子に接続されており、他方の入力端子はインバータ160を介してデータ信号Dの入力端子に接続されている。ORゲート152の出力端子は、2入力NANDゲート153の一方の入力端子に接続されている。NANDゲート153の出力端子は、NANDゲート151の残りの入力端子、NチャンネルMOSトランジスタ158のドレイン電極、及び、2入力ANDゲート156の一方の入力端子に接続される。NチャンネルMOSトランジスタ158のゲート電極にはリセット端子が接続されている。NORゲート155の出力端子は、データQの出力端子、及び、NORゲート157の入力端子に接続される。NORゲート157の出力端子は、データQの反転信号QBの出力端子、及び、NORゲート155の入

力端子に接続される。

【0053】上記構成のフリップフロップ113において、電源投入時に出力するデータの値に影響を与える構成要素であるNANDゲート151及び153は、同一のドライブ能力のものを採用する。また、当該NANDゲート151と153の出力端子に接続される配線容量が同一となるように、NANDゲート151と153の出力端子に接続される配線長を同一に設計すると共に、リセット端子の接続されるNチャンネルMOSトランジスタ158により配線に付加される容量を補償するためMOSトランジスタ158と同一規格のMOSトランジスタ159を対応箇所設ける。これにより、電源投入時にフリップフロップ113から出力端子Dに出力される信号の値が”H”又は”L”である確率を50%にすることができる。

【0054】ランダムビット生成回路110では、上記フリップフロップ113と同じ構成のフリップフロップを2ビットシフトレジスタ115、25ビットシフトレジスタ122及び20ビットシフトレジスタ123にも採用する。これにより、非接触ICカード100の起動時に各シフトレジスタから偏りの無い初期値が出力されるため、乱数データの予測を一層難しくすることができる。

#### 【0055】(5) 乱数生成処理

以下、上記構成の乱数生成回路110を用いてCPU103の実行する乱数生成処理の内容について説明する。図8は、乱数生成処理のフローチャートである。まず、アドレス15F0Hのbit0のデータb0を”0”にセットする(ステップS5)。これにより、クロック発生回路130からのクロック信号CLKの出力が停止し、これに伴いランダムビット生成回路110の動作が停止する。アドレス15F2H~15F7Hを選択し、対応するアドレス信号線を”L”から”H”に切り換え、データD<sub>1</sub>0~D<sub>1</sub>15、D<sub>2</sub>0~D<sub>2</sub>15、D<sub>3</sub>0~D<sub>3</sub>15を乱数データとして読み出す(ステップS6)。更に別の乱数が必要な場合(ステップS7でYES)、アドレス15F0Hのbit0のデータb0を”1”にセットして、ランダムビット生成回路110を起動させた後に(ステップS8)、上記ステップS5に戻る。これ以上の乱数が不要の場合には(ステップS7でNO)、処理を終了する。上記乱数生成処理を実行することで、CPU103は、乱数生成回路110において所定のタイミングで生成された乱数データを抽出することができる。

#### 【0056】(6) テスト処理

上述するように、乱数生成回路107は、システムバス170を流れるデータを利用して規則性の無い予測の困難な乱数を生成することの特徴とする。ところで、所定の周波数のクロック信号CLKが入力されている状態において、ランダムビット生成回路110をリセットした

後に、非接触 I C カード 1 0 0 のテスト処理を実行した場合を想定する。回路が正常な場合には、テスト処理の実行直後にランダムビット生成回路 1 1 0 から出力される乱数データは常に一定の値となる。当該特性を利用すれば、乱数生成回路 1 0 7 を非接触 I C カード 1 0 0 の動作テスト装置として利用することができる。乱数生成回路 1 0 7 をテスト装置として利用することで、テスト専用の回路を不要にして非接触 I C カード 1 0 0 の小型化を図ることができる。

【 0 0 5 7 】 図 9 は、CPU 1 0 3 がランダムビット生成回路 1 1 0 を利用して行うテスト処理のフローチャートである。まず、クロック発生回路 1 3 0 の PLL 回路 1 3 3 に電源回路 1 8 0 から供給される電圧供給信号の電位が規定値  $V_{cc}$  に安定し、所定の周波数のクロック信号 CLK が安定して出力される状態で、アドレス 1 5 F 0 H の b i t 0 のデータ b 0 を " 0 " にセットして、クロック発生回路 1 3 0 の動作を停止、即ち、ランダムビット回路 1 1 0 の動作を停止する (ステップ S 1 0 ) 。アドレス 1 5 F 1 H にダミーデータを書き込み、書き込み命令 W の値を " L " から " H " に切り換え、リセット回路 1 4 0 を機能して各シフトレジスタ 1 1 1 , 1 1 5 , 1 2 2 , 1 2 3 内のデータ (アドレス 1 5 F 2 H ~ 1 5 F 7 H のデータ) をクリアする (ステップ S 1 1 ) 。 1 5 F 0 H の b i t 0 のデータ b 0 を " 1 " にセットして、クロック発生回路 1 3 0 を始動させる (ステップ S 1 2 ) 。ROM 1 0 4 に記憶するテスト用プログラムを実行する (ステップ S 1 3 ) 。テスト用プログラムの実行完了後、アドレス 1 5 F 0 H の b i t 0 のデータ b 0 を " 0 " にセットし、クロック発生回路 1 3 0 の動作を停止する (ステップ S 1 4 ) 。アドレス 1 5 F 2 H ~ 1 5 F 7 H を選択して対応するアドレス信号線を " L " から " H " に切り換え、各ビットデータ  $D_i 0 \sim D_i 15$  ,  $D_i 0 \sim D_i 15$  ,  $D_i 0 \sim D_i 15$  を読み出す (ステップ S 1 5 ) 。

【 0 0 5 8 】 内部の回路が正常の場合、上記ステップ S 1 5 において読み出した各ビットデータ  $D_i 0 \sim D_i 15$  ,  $D_i 0 \sim D_i 15$  ,  $D_i 0 \sim D_i 15$  の値は一定の値を示す。そこで、上記ステップ S 1 5 で読み出した各ビットデータの値と各ビットデータの基準値、例えば、前回読み出した各ビットデータの値又は予め記憶している各ビットデータの値との比較を行い、回路内部に何等かの不都合が生じているか否かの判断を行う (ステップ S 1 6 ) 。比較の結果、上記読み出した各ビットデータの値が基準値と同じ場合には正常であると判断して処理を終了する (ステップ S 1 6 で Y E S ) 。一方、上記読み出した各ビットデータが 1 つでも基準値と異なる場合には回路内に異常があると判断し (ステップ S 1 6 で N O ) 、内部データの保護等の異常対策処理 (ステップ S 1 7 ) を実行した後に処理を終了する。

【 0 0 5 9 】 以上に説明するように、乱数生成回路 1 0

7 は、システムバス 1 7 0 を介して入力されるアドレス信号、データ信号などの各ビットデータの値を利用して乱数を生成するため、規則性の無い予測の困難な乱数データを生成することができる。また、シフトレジスタと加算器からなる簡単な構成のランダムビット生成回路 1 1 0 を採用することで、回路の小型化、及び、高速な乱数生成を実現する。更に、上記ランダムビット生成回路 1 1 0 を非接触 I C カード 1 0 0 のテスト装置として利用することで、専用のテスト回路を排除し、非接触 I C カード 1 0 0 の小型化を図ることができる。

【 0 0 6 0 】 なお、リーダ/ライタ 4 0 0 は、非接触 I C カード 1 0 0 の備える乱数生成回路 1 0 7 と同じ構成の乱数生成回路 4 0 7 を備える。このため、リーダ/ライタ 4 0 0 でも上記非接触 I C カード 1 0 0 と同様に、規則性の無い予測の困難な乱数データを迅速に生成することができる。更に、乱数生成回路 4 0 7 の備えるランダムビット生成回路 (図示せず) をリーダ/ライタ 4 0 0 のテスト装置として利用することで、専用のテスト回路を排除し、リーダ/ライタ 4 0 0 の小型化を図ることができる。

【 0 0 6 1 】

【発明の効果】 本発明の第 1 の乱数生成回路は、外部信号線に流れるビットデータを利用して乱数データを生成するため、規則性の無い予測の困難な乱数データを生成することができる。また、当該乱数生成回路は、シフトレジスタをカスケード接続してなる簡単な構成であるため、高速な乱数データの生成が可能である。

【 0 0 6 2 】 本発明の第 2 の乱数生成回路では、クロック発生回路に、基準周波数信号と同じ周波数に収束するまでの間、供給される電源電圧の値により決まる周波数のクロック信号を出力する PLL 回路を用いることで、例えば、当該第 2 の乱数生成回路を内蔵する非接触 I C カードでも、各構成部品のばらつき等により電源供給開始直後に出力される乱数データの値を相異させることができる。

【 0 0 6 3 】 本発明の第 3 の乱数生成回路は、上記第 1 又は第 2 の乱数生成回路において、更に、各シフトレジスタを構成するクロック同期型フリップフロップの電源投入時に出力するデータを " H " とする第 1 構成要素と、" L " とする第 2 構成要素のドライブ能力を同じにし、かつ、上記第 1 及び第 2 構成要素の出力端子に同じ容量の配線及びトランジスタを接続したことで、電源投入時に出力されるデータが " H " 又は " L " である確率を 5 0 % にすることができる。これにより、電源の投入時、各シフトレジスタから偏りの無い初期値が出力され、乱数データの予測を一層難しくすることができる。

【 0 0 6 4 】 本発明の第 4 の乱数生成回路は、上記何れかの乱数生成回路において、更に、必要に応じて、クロック信号の出力を停止又は動作させることができる。これにより、所定のタイミングの乱数データの読み取りが

可能になる。また、必要に応じて各シフトレジスタに格納するビットデータをリセットすることができる。

【0065】本発明の非接触 IC カードは、上記何れかの乱数生成回路を備えることで、規則性の無い予測の困難な乱数データを迅速に取得できるため、対応するリーダ／ライタとの間で高速な通信処理を行うことができる。

【0066】本発明のリーダ／ライタは、上記何れかの乱数生成回路を備えることで、規則性の無い予測の困難な乱数データを迅速に取得できるため、対応する非接触 IC カードとの間で高速な通信処理を行うことができる。

【0067】上記第4の乱数生成回路をテスト装置として利用する本発明のテスト方法を採用すれば、テスト専用の回路が不要となり装置の小型化を図ることができる。

#### 【図面の簡単な説明】

【図1】 リーダ／ライタと非接触 IC カードの利用形態を説明するための図である。

【図2】 リーダ／ライタ及び非接触 IC カードとの間で実行される相互認証処理のシーケンスを示す図である。

【図3】 リーダ／ライタ及び非接触 IC カードのブロック構成図である。

【図4】 電源回路の構成図である。

【図5】 電源回路の出力特性を示すグラフである。

【図6】 ランダムビット生成回路の構成図である。

【図7】 クロック同期型のフリップフロップの構成図である。

【図8】 CPUの実行する乱数生成処理のフローチャートである。

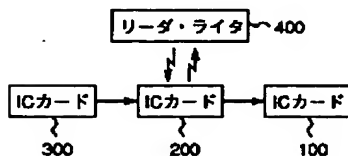
【図9】 CPUの実行するテスト処理のフローチャートである。

【図10】 従来の乱数生成回路の構成図である。

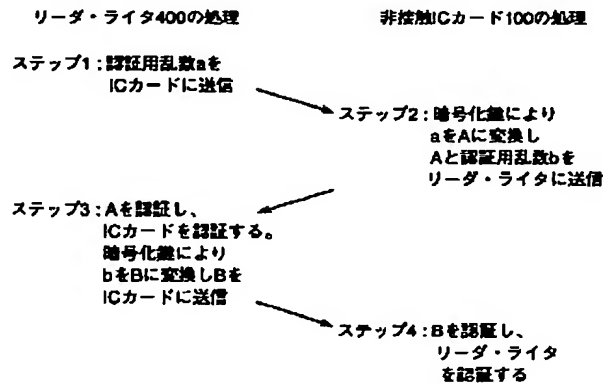
#### 【符号の説明】

100, 200, 300 非接触 IC カード、101, 401 アンテナ、102, 402 送受信回路、103, 403 CPU、104, 404 ROM、105, 405 RAM、106 情報記録部、107, 407 乱数生成回路、108 電源回路、111 1ビットシフトレジスタ、112, 116, 119, 124, 125, 126 加算器、113, 120, 117 フリップフロップ、114, 118, 121 トランスファーマゲート、115 2ビットシフトレジスタ、122 25ビットシフトレジスタ、123 20ビットシフトレジスタ、130 クロック発生回路、131 クロック回路、132 PLL回路、133 NANDゲート、140 リセット回路、141 NANDゲート、150, 152 ORゲート、151, 153 NANDゲート、154, 156 ANDゲート、155, 157 NORゲート、158, 159 トランジスタ、170 システムバス、400 リーダ／ライタ、406 インターフェース

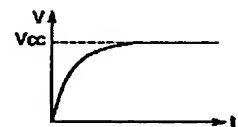
【図1】



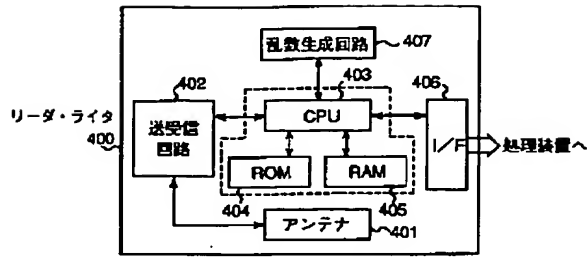
【図2】



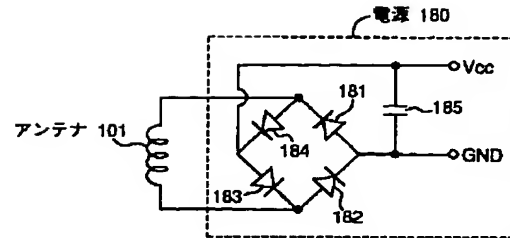
【図5】



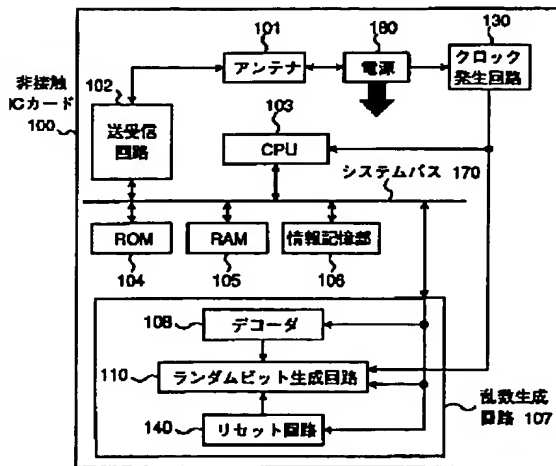
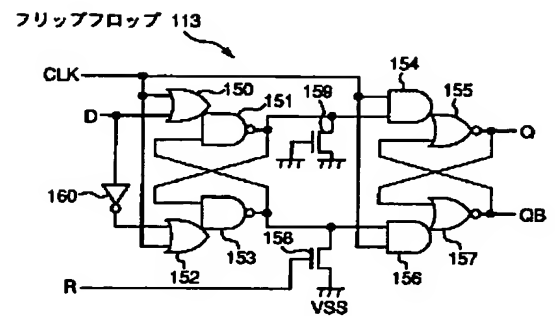
【図 3】



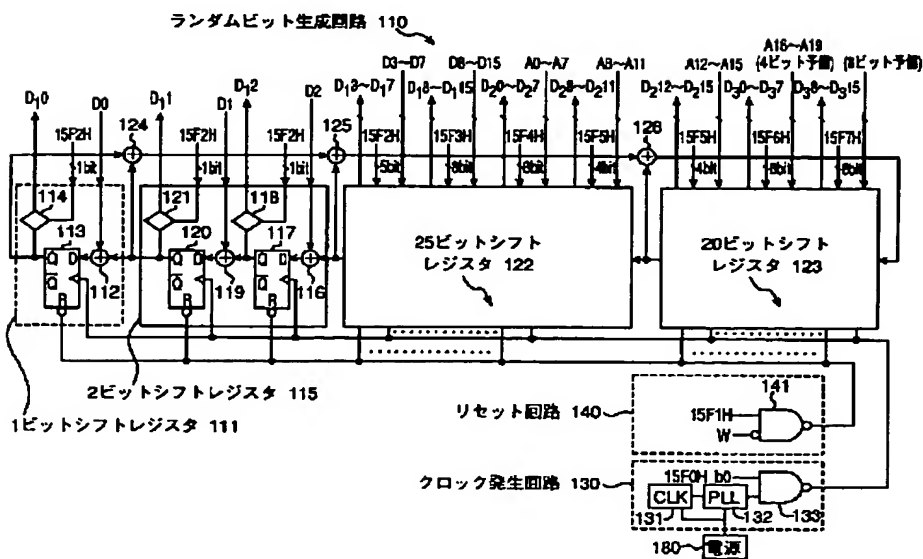
【図 4】



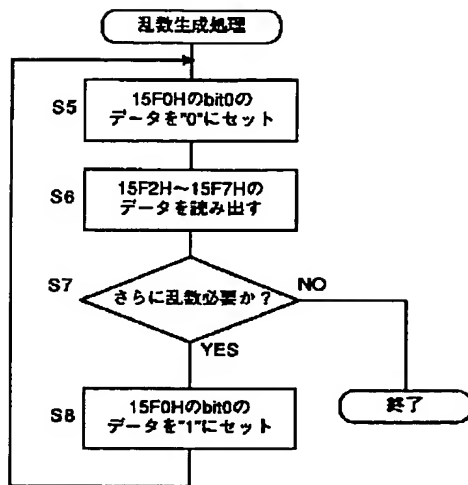
【図 7】



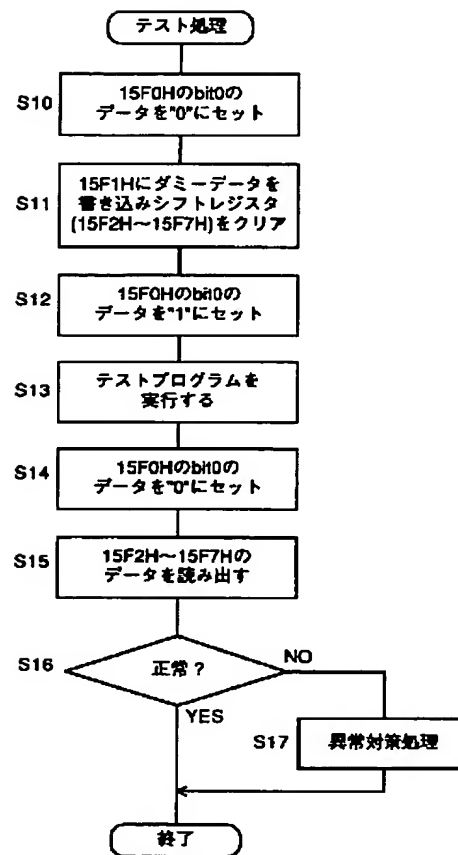
【図 6】



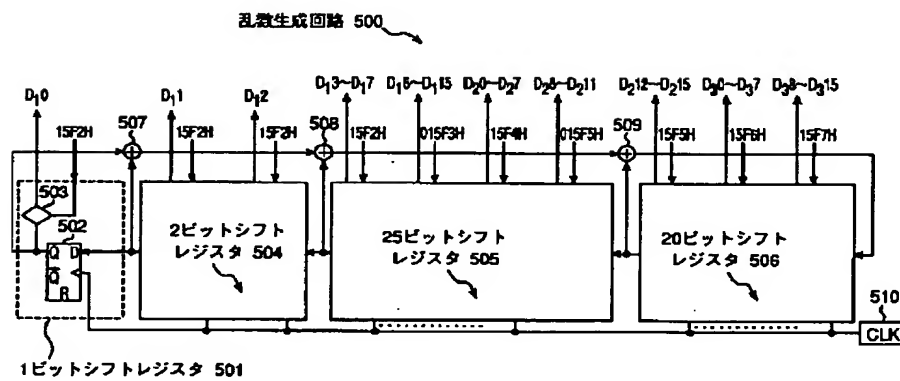
【図 8】



【図 9】



【図 10】



## フロントページの続き

F ターム(参考) 5B035 AA00 AA02 AA03 AA04 AA13  
BB09 BC02 BC03 CA01 CA08  
CA11 CA12 CA22 CA23  
5B058 CA17 CA22 CA27 KA08 KA13  
KA35 YA06 YA07  
5J104 AA18 AA41 FA04 NA23 NA35  
9A001 GG22 LL05

**\* NOTICES \***

**JPO and NCIPi are not responsible for any damages caused by the use of this translation.**

1. This document has been translated by computer. So the translation may not reflect the original precisely.
2. \*\*\*\* shows the word which can not be translated.
3. In the drawings, any words are not translated.

**CLAIMS**

[Claim(s)]

[Claim 1] The circuit which searches for the sum total of the output of two or more shift registers in two or more clock synchronous type shift registers by which cascade connection was carried out, and two or more above-mentioned shift registers, and inputs into the input terminal of the shift register of the first rank the total data for which it asked, It has the clock generation circuit which inputs a clock signal into each above-mentioned shift register. It is the random-number generation circuit which outputs the bit data which each shift register outputs as random-number data. One or more shift register in two or more above-mentioned shift registers The random-number generation circuit characterized by having an adder circuit adding the bit data inputted into an external signal input terminal and one or more bit data in the stored bit data through the above-mentioned external signal input terminal, and outputting the bit data after addition by the adder circuit as random-number data.

[Claim 2] The circuit which searches for the sum total of the output of two or more shift registers in two or more clock synchronous type shift registers by which cascade connection was carried out, and two or more above-mentioned shift registers, and inputs into the input terminal of the shift register of the first rank the total data for which it asked, It has the clock generation circuit which inputs a clock signal into each above-mentioned shift register. It is the random-number generation circuit which outputs the bit data which each shift register outputs as random-number data. The above-mentioned clock generation circuit The random-number generation circuit characterized by consisting of a CLK circuit which generates the clock signal of a predetermined frequency, and a PLL circuit which receives the clock signal generated by the above-mentioned CLK circuit as a reference frequency signal, and outputting the output of the above-mentioned PLL circuit to each above-mentioned shift register.

[Claim 3] In a random-number generation circuit according to claim 1 or 2, the flip-flop of a clock synchronous type which constitutes the above-mentioned shift register It has the same drive capacity as the 1st component which makes "H" the data outputted to a power up, and the 1st component. The random-number generation circuit characterized by having the 2nd component which sets to "L" the data outputted to a power up, and connecting wiring and the transistor of the respectively same capacity to the output terminal of the 1st and 2nd components of the above.

[Claim 4] It is the random-number generation circuit characterized by to have the logical circuit which it has further the reset circuit which outputs a reset signal to each shift register according to the input of a reset demand signal in a random-number generation circuit given in any of claim 1 thru/or claim 3 they are, and the above-mentioned clock-generation circuit suspends the output to each shift register of a clock signal according to the input of a clock stop signal, and outputs a clock signal to each shift register according to the input of a clock actuating signal.

[Claim 5] The noncontact IC card characterized by connecting to the above-mentioned external signal input terminal the predetermined signal line which is the noncontact IC card which contains a random-number generation circuit given in any of claim 1 thru/or claim 4 they are, is equipped with the control means which performs communications processing between the reader/writers for noncontact IC cards concerned using the random-number data outputted from the above-mentioned random-number generation circuit which carries out built-in, and is used by the above-mentioned control means.

[Claim 6] Reader/writer for noncontact IC cards which is the reader/writer for noncontact IC cards which builds in a random-number generation circuit given in any of claim 1 thru/or claim 4 they are, and is

characterized by to connect to the above-mentioned external signal input terminal the predetermined signal line which is equipped with the control means which performs communications processing using the random-number data outputted from the above-mentioned random-number generation circuit which carries out built-in, and is used by the above-mentioned control means between corresponding noncontact IC cards.

[Claim 7] Build in a random-number generation circuit according to claim 4, and it has the control means which performs predetermined processing using the random-number data outputted from the random-number generation circuit concerned to build in. In the condition that the predetermined signal line used by the above-mentioned control means is the test approach of the equipment connected to the above-mentioned external signal input terminal, and the clock signal of a predetermined frequency is outputted from the clock generation circuit After outputting a clock stop signal to the logical circuit of a clock generation circuit and outputting a reset demand signal to a reset circuit Test processing of the above-mentioned equipment is performed at the same time it outputs a clock actuating signal to the logical circuit of a clock generation circuit. The test approach of the equipment which reads the value of the random-number data which output a clock stop signal to completion and coincidence of the above-mentioned test processing in the logical circuit of a clock generation circuit, and are outputted from an output means, and is characterized by performing malfunction detection of a system by the comparison with the random-number data and criteria data which were read.

---

[Translation done.]

## \* NOTICES \*

JPO and NCIPi are not responsible for any damages caused by the use of this translation.

1. This document has been translated by computer. So the translation may not reflect the original precisely.
2. \*\*\*\* shows the word which can not be translated.
3. In the drawings, any words are not translated.

---

DETAILED DESCRIPTION

---

[Detailed Description of the Invention]

[0001]

[Field of the Invention] This invention relates to a random-number generation circuit and the random-number generation circuit especially used for the reader/writer of a noncontact IC card and the noncontact IC card concerned.

[0002]

[Description of the Prior Art] In recent years, many thin noncontact IC cards equipped with an intelligent function or a rewritable memory function are offered. A noncontact IC card is characterized by the ability to perform an exchange of data, without making it connect with reader/writer. A noncontact IC card is used for commuter passes, such as a prepaid card, a key of a door, an electric car, and a bus, the lift ticket of skiing, etc.

[0003] In order to prevent the unjust outflow and alteration of data which are written in the noncontact IC card, the reader/writer of the above-mentioned noncontact IC card and the card concerned performs processing which attests each other, before exchanging data. Reader/writer performs mutual recognition processing between the noncontact IC cards which have answered a letter in the predetermined response signal to the polling signal which self sends. The approach using an encryption key as the approach of mutual recognition processing is learned.

[0004] Hereafter, the mutual recognition processing using the code performed between a noncontact IC card and reader/writer is explained briefly. First, reader/writer transmits the random number a generated inside to the noncontact IC card. A noncontact IC card changes the received random number a into a random number A using the encryption key of self, and returns a random number A to reader/writer. reader/writer -- \*\*\*\* -- specification -- a noncontact IC card -- between -- using -- being common -- encryption -- a key -- using -- the above -- generation -- having carried out -- a random number -- a -- processing -- a random number -- A -- ' -- asking -- having asked -- a random number -- A -- ' -- the above -- a noncontact IC card -- from -- returning -- having had -- a random number -- A -- comparing . Reader/writer attests the noncontact IC card concerned with it being the thing of normal, when a random number A and random-number A' are in agreement.

[0005] Next, a noncontact IC card transmits the random number b generated inside to reader/writer. In this case, reader/writer changes the received random number b into a random number B using the encryption key of self, and returns a random number B to a noncontact IC card. a noncontact IC card -- specification -- reader/writer -- between -- using -- being common -- encryption -- a key -- using -- the above -- generation -- having carried out -- a random number -- b -- processing -- a random number -- B -- ' -- asking -- having asked -- a random number -- B -- ' -- the above -- reader/writer -- from -- returning -- having had -- a random number -- B -- comparing . A noncontact IC card attests the reader/writer concerned with it being the thing of normal, when a random number B and random-number B' are in agreement.

[0006] In a noncontact IC card and reader/writer, the random-number generation circuit which generates the random number used by the above-mentioned mutual recognition processing is built in. Drawing 10 is a circuit diagram of the random-number generation circuit 500 used conventionally. The random-number generation circuit 500 is a circuit called the so-called 48-bit M sequence random-number generation circuit, and consists of adders 507, 508, and 509 which constitute the adder circuit which inputs the sum total of the output of each bit shift register into the input terminal of 20 bit-shift register 506 of the first rank at 1 bit-shift register 501 by which cascade (multistage serial) connection was made, 2 bit-shift register 504, 25 bit-shift

register 505 and 20 bit-shift register 506, and a list.

[0007] 1 bit-shift register 501 is constituted by the flip-flop 502 and the transfer gate 503 which operate synchronizing with the clock signal CLK outputted from the CLK circuit 510. When address 02E2H are chosen by CPU which is not illustrated and an address signal line switches from "L" to "H", the output of a flip-flop 502 is outputted as random-number data D10.

[0008] The circuit of 2 bit-shift register 504, 25 bit-shift register 505, and 20 bit-shift register 506 connects to a serial the circuit as the above-mentioned 1 bit-shift register 501 where only the number of bits shifted respectively is the same. 2 bit-shift register 504 outputs the random-number data D11 and D12, when address 15F2H are chosen. 25 bit-shift register 505 outputs the random-number data D13-D17, D18-D115, D20-D27, and D28-D211, when address 15F2H, 15F3H, 15F4H, and 15F5H are chosen. 20 bit-shift register 506 outputs the random-number data D212-D215, D30-D37, and D38-D315, when address 15F5H, 15F6H, and 15F7H are chosen.

[0009]

[Problem(s) to be Solved by the Invention] The random number which the random-number generation circuit 500 of the above-mentioned configuration generates has the predetermined generation pattern repeated a fixed period. For this reason, the commo data exchanged between reader/writer and a noncontact IC card may be intercepted, and the generation pattern of a random number may be specified. Thus, if the generation pattern of a random number is specified, a noncontact IC card can be forged by using the table on which neither an encryption key nor the contents of encryption processing was understood, but \*\* also matched the random number a and the random number A. Reader/writer can be forged by similarly using the table which matched the random number b and the random number B.

[0010] In order to prevent effectively forgery of the noncontact IC card by tapping of the above-mentioned commo data, or reader/writer, a random-number generation circuit advanced even if it intercepts commo data, like a generation pattern is undecipherable is required. However, the size of a circuit will become large, although unjust decode of a random-number generation pattern can be effectively prevented if a random-number generation circuit is complicated. Especially in the case of a noncontact IC card, the smaller one of the size of the random-number generation circuit to build in is desirable.

[0011] A noncontact IC card needs to complete communications processing including mutual recognition processing, while being in the field in which reader/writer and a communication link are possible. For this reason, activation of communications processing more nearly high-speed than the IC card used inserting in a slot is required. Moreover, in the case of a noncontact IC card, two or more noncontact IC cards may enter at coincidence in the field in which reader/writer and a communication link are possible. In this case, each noncontact IC card needs to perform processing which avoids the collision with the response signal outputted from other noncontact IC cards, such as outputting the response signal over the polling signal from reader/writer before activation of communications processing including the above-mentioned mutual recognition processing to the timing based on the random number generated inside. In order to improve the transmission speed between a noncontact IC card and reader/writer, the random-number generation circuit which operates at high speed is required.

[0012] This invention aims at offering the noncontact IC card which contains the random-number generation circuit which generates the difficult random-number data of the prediction which contributes to the miniaturization of the equipment which contains the circuit concerned with an easy configuration, and does not have regularity in a high speed, and the random-number generation circuit concerned, and the reader/writer for the noncontact IC cards which contain the random-number generation circuit concerned.

[0013]

[Means for Solving the Problem] Two or more clock synchronous type shift registers with which cascade connection of the 1st random-number generation circuit of this invention was carried out, The circuit which searches for the sum total of the output of two or more shift registers in two or more above-mentioned shift registers, and inputs into the input terminal of the shift register of the first rank the total data for which it asked, It has the clock generation circuit which inputs a clock signal into each above-mentioned shift register. It is the random-number generation circuit which outputs the bit data which each shift register outputs as random-number data. One or more shift register in two or more above-mentioned shift registers It has an adder circuit adding the bit data inputted into an external signal input terminal and one or more bit data in the stored bit data through the above-mentioned external signal input terminal, and is characterized by outputting

the bit data after addition by the adder circuit as random-number data.

[0014] Two or more clock synchronous type shift registers with which cascade connection of the 2nd random-number generation circuit of this invention was carried out, The circuit which searches for the sum total of the output of two or more shift registers in two or more above-mentioned shift registers, and inputs into the input terminal of the shift register of the first rank the total data for which it asked, It has the clock generation circuit which inputs a clock signal into each above-mentioned shift register. It is the random-number generation circuit which outputs the bit data which each shift register outputs as random-number data. The above-mentioned clock generation circuit It consists of a CLK circuit which generates the clock signal of a predetermined frequency, and a PLL circuit which receives the clock signal generated by the above-mentioned CLK circuit as a reference frequency signal, and is characterized by outputting the output of the above-mentioned PLL circuit to each above-mentioned shift register.

[0015] The flip-flop of a clock synchronous type with which the 3rd random-number generation circuit of this invention constitutes the above-mentioned shift register in the above 1st or the 2nd random-number generation circuit It has the 1st component which makes "H" the data outputted to a power up, and the 2nd component which sets to "L" the data which have the same drive capacity as the 1st component, and are outputted to a power up. It is characterized by connecting wiring and the transistor of the respectively same capacity to the output terminal of the 1st and 2nd components of the above.

[0016] The 4th random-number generation circuit of this invention is further equipped with the reset circuit which outputs a reset signal to each shift register according to the input of a reset demand signal in the above 1st thru/or which [ 3rd ] random-number generation circuit, the above-mentioned clock generation circuit suspends the output to each shift register of a clock signal according to the input of a clock stop signal, and it is characterized by to have the logical circuit which outputs a clock signal to each shift register according to the input of a clock actuating signal.

[0017] The noncontact IC card of this invention is a noncontact IC card which contains the above 1st thru/or which [ 4th ] random-number generation circuit, is equipped with the control means which performs communications processing between the reader/writers for noncontact IC cards concerned using the random-number data outputted from the above-mentioned random-number generation circuit which carries out built-in, and is characterized by connecting to the above-mentioned external signal input terminal the predetermined signal line used by the above-mentioned control means.

[0018] The reader/writer of this invention is reader/writer for noncontact IC cards which carries out the internal organs of the above 1st thru/or which [ 4th ] random-number generation circuit, and is characterized by connecting to the above-mentioned external signal input terminal the predetermined signal line which is equipped with the control means which performs communications processing using the random-number data outputted from the above-mentioned random-number generation circuit which carries out built-in, and is used by the above-mentioned control means between corresponding noncontact IC cards.

[0019] Carry out the internal organs of the random-number generation circuit of the above 4th, and it has the control means which performs predetermined processing using the random-number data outputted from the random-number generation circuit concerned to build in. While the predetermined signal line used by the above-mentioned control means is the test approach of the equipment connected to the above-mentioned external signal input terminal and outputs a clock stop signal to the logical circuit of a clock generation circuit After outputting a reset demand signal to a reset circuit, test processing of the above-mentioned equipment is performed at the same time it outputs a clock actuating signal to the logical circuit of a clock generation circuit. Read the value of the random-number data which output a clock stop signal to completion and coincidence of the above-mentioned test processing in the logical circuit of a clock generation circuit, and are outputted from an output means, and by the comparison with the random-number data and criteria data which were read Malfunction detection of a system is performed and the above-mentioned random-number generation circuit which carries out built-in is used as a test circuit. Thereby, the circuit only for tests can be made unnecessary and the miniaturization of equipment can be attained.

[0020]

[Embodiment of the Invention] The noncontact IC card which contains the random-number generation circuit concerning the gestalt of operation and the random-number generation circuit concerned hereafter, and the reader/writer for the noncontact IC cards which contain the random-number generation circuit concerned are explained referring to an attached drawing.

[0021] (1) Assume adopting as the automatic wicket system of a subway the noncontact IC card which contains the random-number generation circuit concerning the gestalt of noncontact IC card book operation. As shown in drawing 1, more specifically, the case where those who have the noncontact IC card 100,200,300 which has a function as a commuter pass or a coupon ticket pass through the reader/writer 400 front which functions as an automatic ticket gate in order is assumed. In case reader/writer 400 passes through a front, it recognizes in order the noncontact IC card 100,200,300 which enters in a communications area, when the information about the classification of a commuter pass or a coupon ticket and a card are commuter passes and information, such as an expiration date, and a card are coupon tickets, it reads information, such as the remaining number of sheets, and it updates the information on each card further if needed.

[0022] (2) The authentication reader/writer 400 of a noncontact IC card performs mutual recognition processing between the noncontact IC cards which have answered a letter in the predetermined response signal to the polling signal which self sends. Drawing 2 is drawing showing the sequence of the mutual recognition processing performed between a noncontact IC card 100 and reader/writer 400. First, the random number a for authentication generated by the random-number generation circuit built in from reader/writer 400 to a noncontact IC card 100 is transmitted (step S1). The noncontact IC card 100 which received the random number a for authentication in the communications area changes a random number a into a random number A using the encryption key of self, and the random number b for authentication which generated the random number A by the random-number generation circuit to build in while answering a letter to reader/writer 400 is transmitted (step S2). Reader/writer 400 changes a random number a into random-number A' using the noncontact IC card to access and the encryption key used in common, and when the random number A answered from random-number A' and a noncontact IC card 100 is in agreement, it attests a noncontact IC card 100. Moreover, the random number b transmitted from the noncontact IC card 100 is changed into a random number B using the encryption key of self, and a letter is answered to a noncontact IC card 100 in a random number B (step S3). A noncontact IC card 100 changes a random number b into random-number B' using the reader/writer to access and the encryption key used in common, and reader/writer 400 is attested when the random number B to which it has been answered as random-number B' is in agreement (step S4).

[0023] (3) A noncontact IC card and the block diagram 3 of reader/writer are a noncontact IC card 100 and a block block diagram of reader/writer 400. In addition, the configuration of a noncontact IC card 200,300 is the same as a noncontact IC card 100, and the duplicate explanation is omitted.

[0024] A noncontact IC card 100 is a cell loess type noncontact IC card. A power circuit 180 supplies the signal acquired by an antenna's 101 receiving the RF signal transmitted from reader/writer 400, and rectifying the received RF signal to each internal circuitry which includes the clock generation circuit 130 as a supply signal of an electrical potential difference Vcc. The configuration of a power circuit 180 is explained later.

[0025] The clock generation circuit 130 is driven with the electrical potential difference Vcc supplied from the above-mentioned power circuit 180, and is outputted to CPU103 which is arithmetic and program control about a clock signal CLK, the random bit generation circuit 110 which constitutes the random-number generation circuit 107, and other circuit elements. The configuration of the clock generation circuit 130 is explained later.

[0026] The transceiver circuit 102, ROM104 and RAM105, the information storage section 106, and the random-number generation circuit 107 are connected to CPU103 through the system bus 170. It connects with the antenna 101, and the transceiver circuit 102 performs processing which extracts an instruction and data from the RF signal received through the antenna 101, and is outputted to CPU103 while sending outside the RF signal which carried the instruction sent from CPU103, and data through an antenna 101. ROM104 stores the program which performs communications processing, such as mutual recognition processing with reader/writer 400. RAM105 is used at the time of activation by CPU103 of the program stored in ROM104. The information Records Department 106 holds the information on propers, such as an expiration date of a card, and effective entrainment area, when the original information 100, for example, a noncontact IC card, functions as commuter passes. CPU103 updates information memorized to the above-mentioned information Records Department 106 if needed with activation of communications processing with reader/writer 400. The random-number generation circuit 107 outputs the random-number data used by mutual recognition processing with reader/writer 400 etc. according to selection of the predetermined address by CPU103 to the above CPU 103.

[0027] The random-number generation circuit 107 consists of a decoder 108, a random bit generation circuit 110, and a reset circuit 140. A decoder 108 decodes the data of an address signal inputted through the system bus 170 of CPU103, and outputs them to the random bit generation circuit 110. The random bit generation circuit 110 is inputted in order that the data of an address signal which flow to a system bus 170, the data of a data signal, and the data of other signals may complicate the random-number data generated inside, and when the predetermined address is chosen through the above-mentioned decoder 108, it outputs 3 bytes (48 bits) of random-number data to CPU103 in total. A reset circuit 140 outputs a predetermined reset signal to the random bit generation circuit 110 according to control of CPU103. In addition, the configuration of the random bit generation circuit 110 and a reset circuit 140 is explained in detail later.

[0028] Reader/writer 400 consists of the transceiver circuit 402 which transmits and receives the RF signal in which an instruction and data appeared using the antenna 401 and the above-mentioned antenna 401, CPU403 which is arithmetic and program control, RAM405 used at the time of the program execution by ROM404 and CPU403 which store the communications program including mutual recognition processing with the above-mentioned noncontact IC card 100, an interface 406, and a random-number generation circuit 407. In addition, the random-number generation circuit 407 is the same configuration as the random-number generation circuit 107 built in a noncontact IC card 100.

[0029] In reader/writer 400, CPU403 which is arithmetic and program control is connected to the transceiver circuit 402, ROM404 and RAM405, the interface 406, and the random-number generation circuit 407 through the system bus. The transceiver circuit 402 sends the high frequency signal which carried the instruction and data from CPU403 through an antenna 401 while it extracts an instruction and data from the high frequency signal received through the antenna 401 connected and outputs them to CPU403. The random-number data with a noncontact IC card 100 obtained from the random-number generation circuit 407 at the time of activation of mutual recognition processing are used for CPU403. CPU403 outputs the result of communications processing to each processor through an interface 406.

[0030] Drawing 4 is drawing showing the configuration of a power circuit 180. A power circuit 180 is constituted from capacity 185 by the diodes 181, 182, 183, and 184 and the list which constitute a rectifier circuit. The rectifier circuit concerned rectifies the RF signal inputted through an antenna 101, and outputs it to each internal circuitry by making the signal after the rectification concerned into an electrical-potential-difference supply signal.

[0031] Drawing 5 is a graph which shows change of the potential of the electrical-potential-difference supply signal outputted from a power circuit 180 from reception initiation of the RF signal from reader/writer 400. In order for the potential of the electrical-potential-difference supply signal outputted from a power circuit 180 to become default value Vcc so that it may illustrate, after starting reception of a RF signal, predetermined time amount is required. In addition, the time amount taken for the potential of an electrical-potential-difference supply signal to serve as Vcc changes with communication environment with reader/writer 400.

[0032] (4) The random-number generation circuit diagram 6 is drawing showing the detailed configuration of the clock generation circuit 130 in the random bit generation circuit 110 built in the random-number generation circuit 107 and a reset circuit 140, and a list.

[0033] (4-1) The random bit generation circuit random bit generation circuit 110 1 bit-shift register 111 which constitutes the so-called 48-bit M sequence random-number generation circuit, 2 bit-shift register 115, and 25 bit-shift register 122 -- and On the bit data and the concrete target which change with the contents of the processing which CPU103 performs to each bit data stored in 20 bit-shift register 123 with time amount each bit data A0-A19 of the 20-bit address signal which passes along a system bus 170, and each bit data D0-D15 of a 16-bit data signal -- and It is characterized by adopting a total of the bytes [ 3 bytes which adds respectively a total of each 12-bit bit data which consist of other signals, and is added and obtained ], i.e., 48 bits, data D10-D115, D20-D215, and the configuration that outputs D30-D315 as random-number data.

[0034] By adopting the above-mentioned configuration, the difficult random-number data of irregular prediction are generable. Even if this intercepts the commo data performed between a noncontact IC card 100 and reader/writer 400, it becomes difficult to specify the generation pattern of a random number, and forgery of a noncontact IC card can be prevented effectively. Moreover, since the easy configuration which connected the shift register and the adder (EXOR gate) is used for the random bit generation circuit 110, it can generate a high-speed random number.

[0035] Hereafter, it explains in full detail about the configuration of the random bit generation circuit 110.

The random bit generation circuit 110 consists of three adders 124, 125, 126 which constitute the circuit which outputs the sum total of the output of each shift register to 20 bit-shift register 123 of the first rank at 1 bit-shift register 111 by which cascade (multistage serial) connection was made, 2 bit-shift register 115, 25 bit-shift register 122 and 20 bit-shift register 123, and a list.

[0036] The input terminal of 20 bit-shift register 123 is connected to the output terminal of an adder 126. The output terminal of 20 bit-shift register 123 is connected to the input terminal of an adder 126, and the input terminal of 25 bit-shift register 122. The output terminal of 25 bit-shift register 122 is connected to the input terminal of an adder 125, and the input terminal of 2 bit-shift register 115. The output terminal of 2 bit-shift register 115 is connected to the input terminal of an adder 124, and the input terminal of 1 bit-shift register 111. The output terminal of 1 bit-shift register 111 is connected to the input terminal of an adder 124. The output terminal of an adder 124 is connected to the input terminal of an adder 125. The output terminal of an adder 125 is connected to the input terminal of an adder 126.

[0037] Address 15F2H are chosen through a decoder 108, and 1 bit-shift register 111 outputs the data D10 of bit0 of the data which add the data D0 of bit0 of a 16-bit data signal which flow a system bus 170 to 1 bit data to store, and are obtained as random-number data, when a corresponding address signal line switches from "L" to "H".

[0038] 1 bit-shift register 111 consists of an adder 112, a flip-flop 113, and the transfer gate 114. It consists of the EXOR gates and an adder 112 inputs into a flip-flop 113 the data of bit0 which adds the data D0 of bit0 of 16 bit-data signals inputted into the output of 2 bit-shift register 115 prepared in the preceding paragraph through a system bus 170, and is obtained. A flip-flop 113 is a flip-flop of a clock synchronous type, and operates synchronizing with the transition timing of the clock signal CLK inputted into a clock input terminal. Address 15F2H are chosen, and the transfer gate 114 outputs the output Q of a flip-flop 113 as random-number data D10, when a corresponding address signal line switches from "L" to "H".

[0039] Address 15F2H are chosen through a decoder 108, and 2 bit-shift register 115 outputs the data D11 and D12 adding the data D1 of the data D2 and bit1 of bit2 of 16 bit-data signals inputted into each stored 2-bit bit data through a data bus as random-number data, when a corresponding address signal line switches from "L" to "H".

[0040] 2 bit-shift register 115 connects 1 bit-shift register to a two-step serial so that it may illustrate. That is, the 1st 1 bit-shift register is constituted from an adder 116, a flip-flop 117, and the transfer gate 118, and the 2nd 1 bit-shift register consists of next adders 119, flip-flops 120, and tolan FUFA gates 121. The same is said also of 25 bit-shift register 122 and 20 bit-shift register 123 which are explained below. Since the contents of processing of the signal in each shift register are the same as that of the above-mentioned 1 bit-shift register 111, explanation here is omitted.

[0041] 25 bit-shift register 122 to each stored 25-bit bit data each bit data A0-A11 of bit0-bit11 of a 20-bit address signal inputted through an address bus -- and The 25-bit bit data D13-D17 which add each bit data D3-D15 of bit3-bit15 of a 16-bit data signal inputted through a data bus, and are obtained, D18-D115, D20-D27, and D28-D211 It outputs according to selection of address 15F2H, 15F3H, 15F4H, and 15F5H.

[0042] 20 bit-shift register 123 to each 20-bit bit data stored each bit data Rev0-Rev7 of each 8-bit bit data bit0-bit7 which consist of signals other than a data signal and an address signal -- and The 20-bit data D212-D215 adding each bit data A12-A19 of bit12-bit19 of a 20-bit address signal inputted through an address bus, D30-D37, and D38-D315 It outputs according to selection of address 15F5H, 15F6H, and 15F7H.

[0043] In the random bit generation circuit 110, the configuration adding each bit data which constitute the address signal and data signal which flow a system bus 170, and other signals is adopted to each bit data stored in each bit shift register 111, 115, 122 and 123 so that it may mention above. Since the value of the signal which flows to a system bus 170 changes variously in connection with the contents of processing to perform, it can generate the difficult random-number data of irregular prediction. Even if this intercepts the commo data exchanged between a noncontact IC card 100 and reader/writer 400, it becomes difficult to specify the generation pattern of a random number, and it can prevent forgery of a noncontact IC card effectively. Moreover, since the random bit generation circuit 110 is the easy configuration which connected the shift register and the adder (EXOR gate), it can generate a high-speed random number.

[0044] Although the configuration which inputs into the input terminal of 20 bit-shift register 123 of the first rank the sum total of the output of all shift registers which carried out cascade connection is used for the above-mentioned random bit generation circuit 110, it should just be the configuration of inputting into the

input terminal of 20 bit-shift register 123 of the first rank the sum total of the output of two or more of four shift registers which are not limited to this but constitute the random bit generation circuit 110.

[0045] Moreover, although the configuration which outputs the bit data stored in all shift registers corresponding to selection of the predetermined address by CPU103 as random-number data is used for the random bit generation circuit 110, it should just be a configuration which is not limited to this but outputs one or more bit data.

[0046] Furthermore, although the configuration which adds the bit data of a system bus 170 to all the bit data stored in each shift register is used for the random bit generation circuit 110, it should just be the configuration of adding the bit data of a system bus 170 to one or more bit data in the bit data which it is not limited to this but are stored in a shift register.

[0047] (4-2) The reset circuit reset circuit 140 consists of 2 input NAND gates 141. The address signal line of address 15F1H is connected to the input terminal of NAND gate 141, and when a write-in instruction is issued by the remaining input terminals, W signal line which switches from "L" to "H" is connected. CPU103 can reset each shift register 111, 115, 122, 123 which constitutes the random bit generation circuit 110 from writing in data to address 15F1H.

[0048] (4-3) As shown in the clock generation circuit diagram 6, the clock generation circuit 130 consists of a CLK circuit 131, PLL132, and NAND gate 133. The CLK circuit 131 is outputted to the PLL circuit 132 of the next step by making the clock signal of a predetermined period into a reference frequency signal at the same time an electrical-potential-difference supply signal is outputted from a power circuit 180. As everyone knows, the PLL circuit 132 outputs the clock signal of the frequency decided in proportion to the potential of the electrical-potential-difference supply signal outputted from a power circuit 180 until it converges on the frequency of the above-mentioned reference frequency signal. The output terminal of the PLL circuit 132 is connected to one input terminal of 2 input NAND gate 133. The data b0 of bit0 of address 15F0H after decoding are inputted into another input terminal of NAND gate 133. Usually, the data b0 of address 15F0H are set as "L", and NAND gate 133 outputs the reversal signal of the clock signal CLK from the PLL circuit 131 to each shift registers 111, 115, 122, and 123 which constitute the random bit generation circuit 110.

[0049] The frequency of the clock signal which the clock generation circuit 130 outputs is decided by potential of the electrical-potential-difference supply signal outputted from a power circuit 180 so that it may mention above. For this reason, even if it reads random-number data to the completely same timing until the potential of the electrical-potential-difference supply signal outputted from a power circuit 180 is stabilized in default value Vcc, the values of the random-number data outputted from the random bit generation circuit 110 differ. Moreover, since the reading timing of the above-mentioned random-number data changes delicately with dispersion in each component part even if it is the noncontact IC card 200 of the completely same configuration as a noncontact IC card 100, and 300, the random-number data outputted from the random bit generation circuit 110 immediately after powering on differ for every card. Thus, by adopting the clock generation circuit 130 of the above-mentioned configuration, specification of the generating pattern of the random-number data based on tapping of commo data can be made much more difficult.

[0050] In addition, in the clock generation circuit 130 of the above-mentioned configuration, if the data b0 of bit0 of address 15F0H are rewritten "from L" to "H" by CPU103, NAND gate 133 will output only "H". In this, the output of the clock signal to each shift registers 111, 115, 122, and 123 which constitute the random bit generation circuit 110 stops, and the function of each shift register stops. Moreover, the output of the clock signal to each shift register can be resumed by rewriting the value of the data b0 of bit0 of address 15F0H from "H" to "L." Thus, CPU103 can operate and stop the random bit generation circuit 110.

[0051] (4-4) The clock synchronous type flip-flop 113 which constitutes the flip-flop 1 bit-shift register 111 is characterized by to make the same wiring capacity connected to the output terminal of the 1st and 2nd components of the above while it is equipped with the same drive capacity as the 1st component which makes "H" the data outputted to a power up, and the 1st component of the above and is equipped with the 2nd component which sets to "L" the data outputted to a power up. The probability for the data outputted to a power up to be set to "H" or "L" by this is made 50%.

[0052] Drawing 7 is drawing showing the configuration of a flip-flop 113. One input terminal of 2 input OR gate 150 is connected to the input terminal of a clock signal CLK, and the input terminal of another side is connected to the input terminal of data signal D. The output terminal of the OR gate 150 is connected to one input terminal of 2 input NAND gate 151. The output terminal of NAND gate 151 is connected to the drain

electrode of the N-channel MOS transistor 159 with which one input terminal, gate electrode, and source electrode of 2 input NAND gate 153 are grounded, and one input terminal of 2 input AND gate 154. One input terminal of 2 input OR gate 152 is connected to the input terminal of a clock signal CLK, and the input terminal of another side is connected to the input terminal of data signal D through the inverter 160. The output terminal of the OR gate 152 is connected to one input terminal of 2 input NAND gate 153. The output terminal of NAND gate 153 is connected to the remaining input terminals of NAND gate 151, the drain electrode of the N-channel MOS transistor 158, and one input terminal of 2 input AND gate 156. The reset terminal is connected to the gate electrode of the N-channel MOS transistor 158. The output terminal of the NOR gate 155 is connected to the output terminal of Data Q, and the input terminal of the NOR gate 157. The output terminal of the NOR gate 157 is connected to the output terminal of the reversal signal QB of Data Q, and the input terminal of the NOR gate 155.

[0053] The thing of the same drive capacity is used for NAND gates 151 and 153 which are the components which affect the value of the data outputted to a power up in the flip-flop 113 of the above-mentioned configuration. Moreover, while designing identically the wire length connected to the output terminal of NAND gates 151 and 153 so that the wiring capacity connected to the output terminal of NAND gates 151 and 153 concerned may become the same, in order to compensate the capacity added to wiring by the N-channel MOS transistor 158 to which a reset terminal is connected, MOS transistor 159 of the same specification as MOS transistor 158 is formed in a correspondence part. Thereby, the probability for the value of the signal outputted to a power up from a flip-flop 113 at an output terminal D to be "H" or "L" can be made 50%.

[0054] In the random bit generation circuit 110, the flip-flop of the same configuration as the above-mentioned flip-flop 113 is adopted also as 2 bit-shift register 115, 25 bit-shift register 122, and 20 bit-shift register 123. Since initial value without a bias is outputted from each shift register by this at the time of starting of a noncontact IC card 100, prediction of random-number data can be made much more difficult.

[0055] (5) Explain the contents of the random-number generation processing which CPU103 performs using the random-number generation circuit 110 of the above-mentioned configuration below random-number generation processing. Drawing 8 is the flow chart of random-number generation processing. First, the data b0 of bit0 of address 15F0H are set to "0" (step S5). Thereby, the output of the clock signal CLK from the clock generation circuit 130 stops, and actuation of the random bit generation circuit 110 stops in connection with this. Address 15F2H-15F7H are chosen, a corresponding address signal line is switched to "H" from "L", and data D10-D115, D20-D215, and D30-D315 are read as random-number data (step S6). Furthermore, when another random number is required (it is YES at step S7), the data b0 of bit0 of address 15F0H are set to "1", and after starting the random bit generation circuit 110, it returns to (step S8) and the above-mentioned step S5. When the random number beyond this is unnecessary, NO) and processing are ended at the (step S7). By performing the above-mentioned random-number generation processing, CPU103 can extract the random-number data generated to predetermined timing in the random-number generation circuit 110.

[0056] (6) The random-number generation circuit 107 is characterized by generating the difficult random number of the prediction which is irregular using the data which flow a system bus 170 so that test processing \*\*\*\* may be carried out. By the way, in the condition that the clock signal CLK of a predetermined frequency is inputted, after resetting the random bit generation circuit 110, the case where test processing of a noncontact IC card 100 is performed is assumed. When a circuit is normal, the random-number data outputted from the random bit generation circuit 110 immediately after activation of test processing always serve as a fixed value. If the property concerned is used, the random-number generation circuit 107 can be used as operation-test equipment of a noncontact IC card 100. By using the random-number generation circuit 107 as test equipment, the circuit only for tests can be made unnecessary and the miniaturization of a noncontact IC card 100 can be attained.

[0057] Drawing 9 is the flow chart of the test processing which CPU103 performs using the random bit generation circuit 110. First, the potential of the electrical-potential-difference supply signal supplied to the PLL circuit 133 of the clock generation circuit 130 from a power circuit 180 is stabilized in default value Vcc, and in the condition of being stabilized and outputted, the clock signal CLK of a predetermined frequency sets the data b0 of bit0 of address 15F0H to "0", and suspends a halt, i.e., actuation of the random bit circuit 110, for actuation of the clock generation circuit 130 (step S10). Dummy data is written in address 15F1H, the value of the write-in instruction W is switched to "H" from "L", a reset circuit 140 is functioned, and the

data in each shift register 111,115,122,123 (data of address 15F2H-15F7H) are cleared (step S11). The data b0 of bit0 of 15F0H are set to "1", and the clock generation circuit 130 is started (step S12). The program for a test memorized to ROM104 is performed (step S13). The data b0 of bit0 of address 15F0H are set to "0" after the program execution completion for a test, and actuation of the clock generation circuit 130 is suspended (step S14). The address signal line which chooses address 15F2H-15F7H, and corresponds is switched to "H" from "L", and each bit data D10-D115, D20-D215, and D30-D315 are read (step S15).

[0058] When an internal circuit is normal, the value of each bit data D10-D115 read in the above-mentioned step S15, D20-D215, and D30-D315 shows a fixed value. Then, the comparison with the value of each bit data read at the above-mentioned step S15 and the reference value of each bit data, for example, the value of each bit data read last time, and the value of each bit data memorized beforehand is performed, and it judges whether certain un-arranging has arisen inside the circuit (step S16). as a result of a comparison, when the value of each bit data which carried out [ above-mentioned ] reading appearance is the same as a reference value, it judges that it is normal and processing is ended (it is YES at step S16). processing is ended, after judging that abnormalities are in a circuit (it is NO at step S16) and, performing abnormality cure processing (step S17) of protection of an in-house data etc. on the other hand, when at least each one bit data which carried out [ above-mentioned ] reading appearance differ from a reference value.

[0059] Since the random-number generation circuit 107 generates a random number using the value of each bit data inputted through a system bus 170, such as an address signal and a data signal, it can generate the difficult random-number data of irregular prediction, so that it may explain above. Moreover, miniaturization of a circuit and high-speed random-number generation are realized by adopting the random bit generation circuit 110 of an easy configuration of consisting of a shift register and an adder. Furthermore, by using the above-mentioned random bit generation circuit 110 as test equipment of a noncontact IC card 100, the test circuit of dedication can be eliminated and the miniaturization of a noncontact IC card 100 can be attained.

[0060] In addition, reader/writer 400 is equipped with the random-number generation circuit 407 of the same configuration as the random-number generation circuit 107 with which a noncontact IC card 100 is equipped. For this reason, the irregular difficult random-number data of prediction as well as [ reader/writer 400 ] the above-mentioned noncontact IC card 100 are quickly generable. Furthermore, by using the random bit generation circuit (not shown) with which the random-number generation circuit 407 is equipped as test equipment of reader/writer 400, the test circuit of dedication can be eliminated and the miniaturization of reader/writer 400 can be attained.

[0061]

[Effect of the Invention] Since the 1st random-number generation circuit of this invention generates random-number data using the bit data which flow to the external signal line, it can generate the difficult random-number data of irregular prediction. Moreover, since the random-number generation circuit concerned is an easy configuration which comes to carry out cascade connection of the shift register, generation of high-speed random-number data is possible for it.

[0062] using the PLL circuit which outputs the clock signal of the frequency decided by the value of the supply voltage supplied to a clock generation circuit in the 2nd random-number generation circuit of this invention until it converges on the same frequency as a reference frequency signal -- for example, difference of the value of the random-number data with which the noncontact IC card which contains the 2nd random-number generation circuit concerned is also outputted immediately after current supply initiation by dispersion in each component part etc. can be carried out.

[0063] The 3rd random-number generation circuit of this invention is set in the above 1st or the 2nd random-number generation circuit. Furthermore, the 1st component which makes "H" the data outputted to the power up of the clock synchronous type flip-flop which constitutes each shift register, The probability which is "data outputted to power up by having made the same drive capacity of 2nd component made into L", and having connected wiring and transistor of same capacity as output terminal of 1st and 2nd components of the above" H" or "L" can be made 50%. Thereby, at the time of the injection of a power source, initial value without a bias is outputted from each shift register, and prediction of random-number data can be made much more difficult.

[0064] the 4th random-number generation circuit of this invention -- the above -- in which random-number generation circuit, further, the need can be accepted, and the output of a clock signal can be stopped or operated. Thereby, reading of the random-number data of predetermined timing becomes possible. Moreover,

the bit data stored in each shift register if needed are resettable.

[0065] Since the noncontact IC card of this invention can acquire the difficult random-number data of irregular prediction quickly by having the random-number generation circuit of one of the above, it can perform high-speed communications processing between corresponding reader/writers.

[0066] Since the reader/writer of this invention can acquire the difficult random-number data of irregular prediction quickly by having the random-number generation circuit of one of the above, it can perform high-speed communications processing between corresponding noncontact IC cards.

[0067] If the test approach of this invention of using the random-number generation circuit of the above 4th as test equipment is adopted, the circuit only for tests becomes unnecessary and the miniaturization of equipment can be attained.

---

[Translation done.]

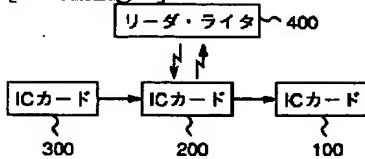
## \* NOTICES \*

JPO and NCIPi are not responsible for any damages caused by the use of this translation.

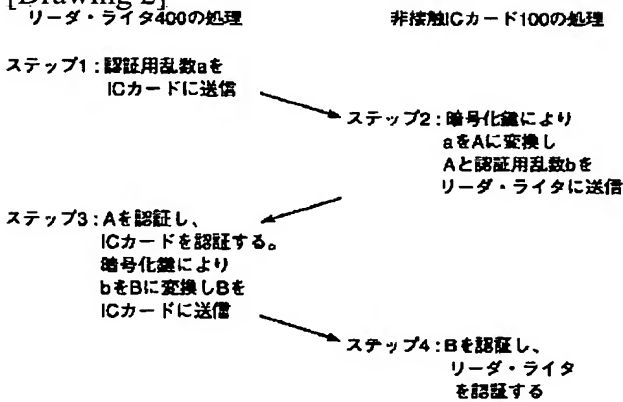
1. This document has been translated by computer. So the translation may not reflect the original precisely.
2. \*\*\*\* shows the word which can not be translated.
3. In the drawings, any words are not translated.

## DRAWINGS

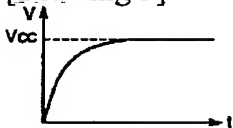
[Drawing 1]



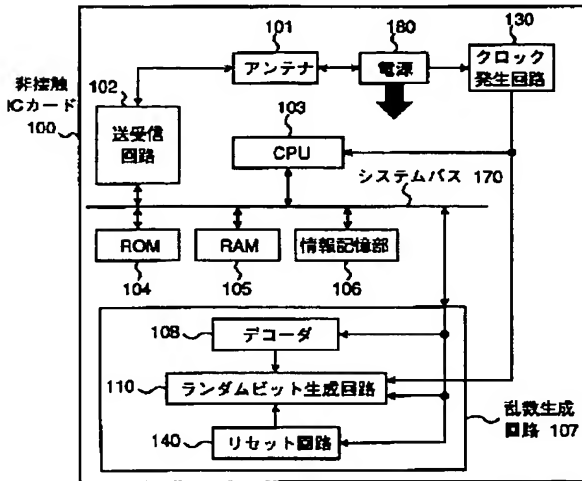
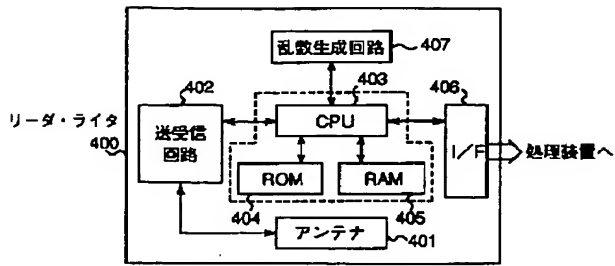
[Drawing 2]



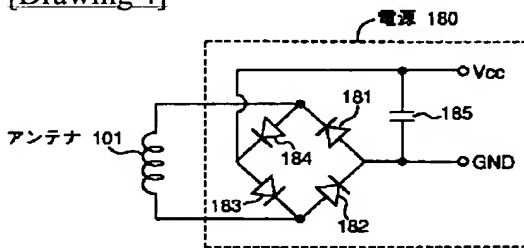
[Drawing 5]



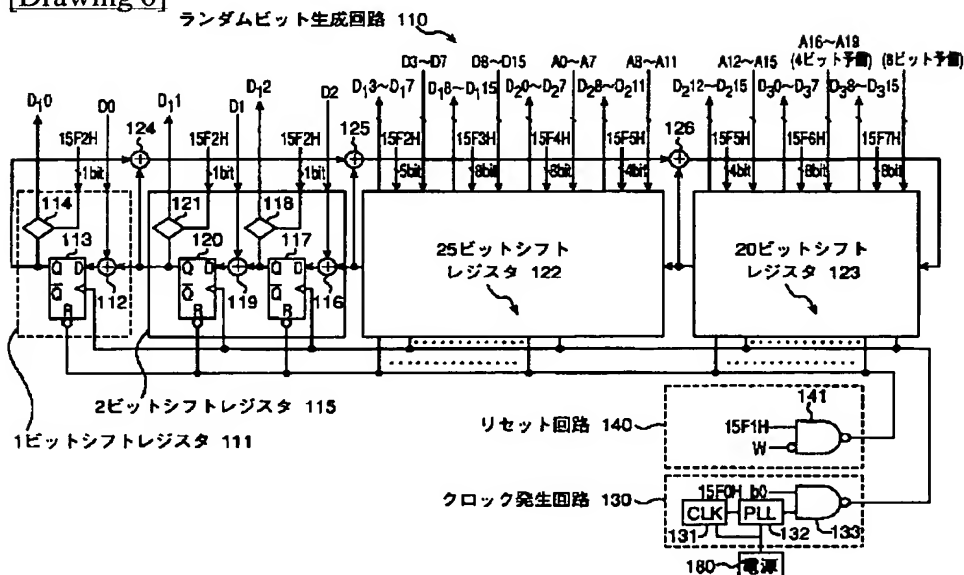
[Drawing 3]



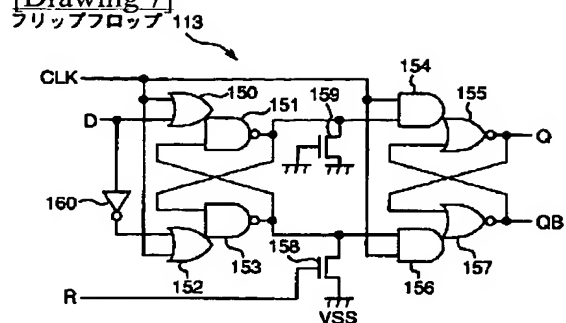
[Drawing 4]



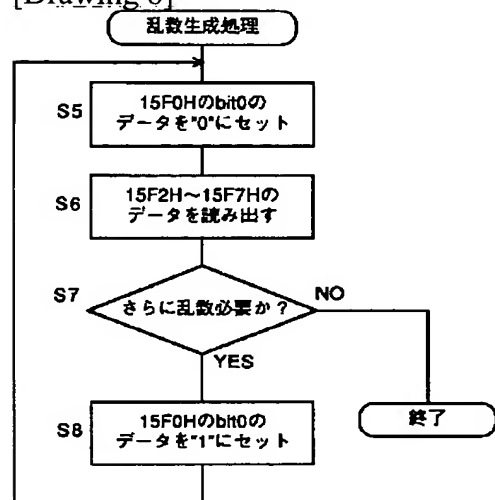
[Drawing 6]



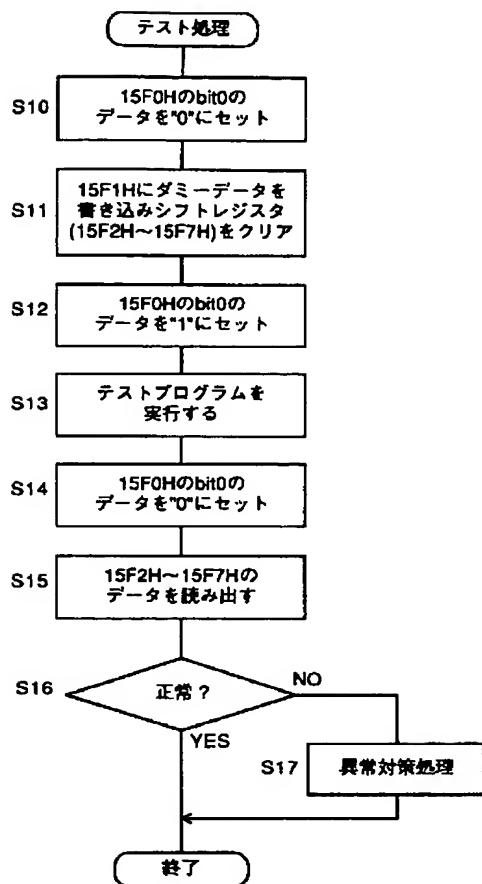
[Drawing 7]



[Drawing 8]

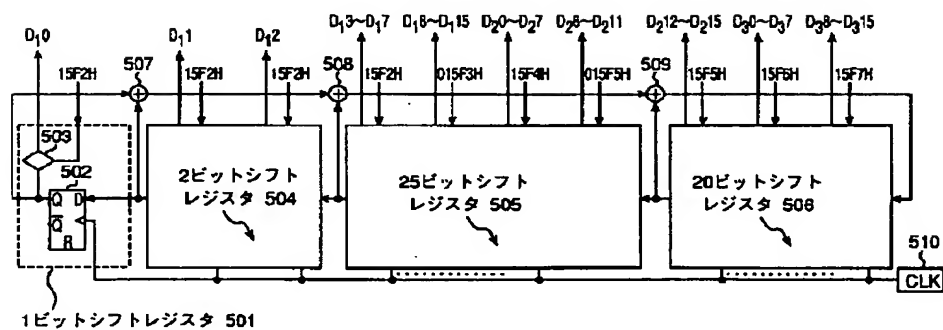


[Drawing 9]



[Drawing 10]

乱数生成回路 500



[Translation done.]